A3SECURITY

에이쓰리시큐리티 회사소개서

2022.11

We make your value secure!

A3SECURITY

01
회사소개

비전 및 경영방침
일반 현황
주요 연혁
인증 내역
수상 내역
주요 고객사

02
사업영역

사업 개요

03
사업소개

보안컨설팅
보안관제

We make your value secure!

A3SECURITY

01

Company Information

회사소개

비전 및 경영방침
일반 현황
주요 연혁 및 수상
주요 고객사
주요 사업 실적 요약

We make your value secure!

We make your value secure!

No.1 Security Service Provider

We design the security on the cyber world!

사이버 세상에 보안을 디자인 한다!

회사명	㈜에이쓰리시큐리티	대표이사	한 재 호
설립일	1999년 08월 16일	임직원수	80명 (2022.11 기준)
소재지	서울 영등포구 선유로9길 10 (문래동6가, 문래 SK V1 center) 1710-11호	사업분야	보안컨설팅 및 서비스 외

㈜에이쓰리시큐리티는 통합 위험관리 전문기업으로 공공, 금융, 통신 및 하이테크, 쇼핑, 게임 등 인터넷을 이용하여 사업을 영위하는 기업을 대상으로 정보보호 체계 및 솔루션 구축을 주된 사업으로 하고 있는 정보보호 분야의 명가 입니다.

4차 산업혁명의 시대에 필수 요소가 된 정보보호 기술 및 관리 분야에 오랜 경험과 노하우를 기반으로,
고객사로 하여금 안전하고 효과적인 경영목적을 달성할 수 있도록 하고 있습니다.

History

1999년 부터 현재까지 지식정보보안 체계 구축을 위한 컨설팅 및 솔루션 구축기반으로 성장 중

2016' – 2021'

A3SECURITY 20th 기념식 개최
ESP(전사적통합정보보호관리시스템) v4.2 출시
에이쓰리시큐리티&오픈시큐어랩 공개보안 세미나 개최
LGCNS와 LG보안포털사업 공동협력
제7회 개인정보보호 페어(PIS FAIR 2017) 참가
SecuCare Service(정보보안관리전문가지원서비스) 출시
미래창조과학부 2016 정보보호 인력채용 박람회 참가

2005' – 2009'

"Rfinder PIA" 개인정보보호솔루션 최초 GS 인증 획득
법무법인 김앤장과 전략적 MOU 체결
방송통신위원회위원장 표창장 수상
A3Security Solution Day 2008개최
KISA 제4회 해킹방어대회 대상
PCI QSA 등록 (국내유일 PCI 보안실사업체)
제 3 회 해킹방지대회 금상 수상
Citrix사와 파트너 계약 체결
기술혁신형중소기업 인증 (INNO-BIZ)
소스코드진단 방법론 자체 개발

2010' – 2015'

"Rfinder CMS" 컴플라이언스관리시스템 런칭
보안관리전략 세미나 SMS 2013 개최
"Rfinder GAIA" 개인정보시스템 런칭
개인정보영향평가 기관 (행정안전부) 지정
보안관제 전문업체 (지식경제부) 지정
지식경제부장관 표창장 수상
한국경제 지식서비스 최우수 기업 수상
보안관제센터 오픈 (관제서비스 AEGIS 론칭)
제9회 정보보호대상 특별상 수상
제9회 대한민국 소프트웨어 보안 SW분야 우수상 수상

1999' - 2004'

제 1 회 해킹방지대회 대상 수상
'실시간 위험지수 산정 방법 및 그 시스템' 특허
1.25 인터넷 대란 관련 정통부 합동조사단 활동
정보보호관리체계(ISMS) 인증 획득
ISO27001(구 BS7799) 인증 획득
기업부설연구소 인증 (한국산업기술진흥협회)
벤처기업 인증 (기술보증기금)
정보보호전문업체 지정 (평가1위, 정보통신부)
회사 설립

Certification & Awards

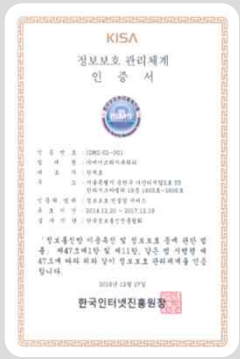
주요 인증 및 수상 내역 입니다.

ISO27001

보안관제전문기업

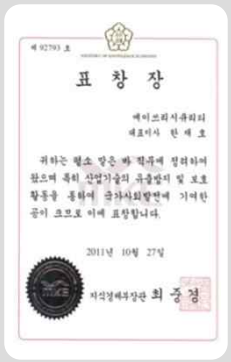
정보보호서비스 전문기업

개인정보 영향평가기관



정보보호관리체계 인증

정보보호대상 특별상



지식경제부 장관표창장

정보보호강화 표창장

대한민국SW경쟁력대상

ISO27001 고도화 표창장

Our Client

20년간 약 2,000건 이상의 풍부한 정보보안프로젝트 수행경험을 갖고 있으며,
많은 기관과 기업에서 에이쓰리시큐리티를 선택 했습니다.

공공

대법원
서울특별시
금융감독원
중앙선거관리위원회
국세청
건강보험심사평가원
한국은행
NPS
나라살림 가치창조 조달청
KISA 한국인터넷진흥원
감사원
경기도교육청
행정안전부
경상남도교육청
청와대
KORES

금융

IBK기업은행
OSB저축은행
KB국민은행
acuon capital
신한은행
삼성카드
SAMSUNG
하나은행
신한카드
우리은행
MIRAE ASSET 미래에셋대우
KDB산업은행
대신증권 Daishin Securities
NH농협은행
MUFG Bank of Tokyo-Mitsubishi UFJ
DGB 대구은행
MERITZ 메리츠종금증권

제조 · 유통

현대홈쇼핑
HYUNDAI MOBIS
HYUNDAI DEPARTMENT STORE
posco
흠&쇼핑
S-OIL 에쓰-오일
GS SHOP
GS 칼텍스주식회사
LG전자
Home plus
LG Display
Gmarket
SAMSUNG 삼성전자
LF
HYUNDAI
Dongwon

IT · 통신

NAVER
Daum
kt sat
CJ 올리브네트웍스
SK 텔레콤
kct
SK broadband
한화시스템
LG U+
LG엔시스
NCSOFT
LG CNS
NEXON
신세계 아이앤씨
kt
koscom

기타

KOREAN AIR
서강대학교
Incheon Airport
KRX 한국거래소
인하대병원
Let's Run 한국마사회
SAMSUNG 삼성서울병원
Ktoto
서울아산병원 Asan Medical Center
Your Best Credit Partner SGI서울보증
국립중앙의료원 National Medical Center
내일을 향한 금융 한화생명
고려대학교의료원 KOREA UNIVERSITY MEDICAL CENTER
DB손해보험
고려대학교 KOREA UNIVERSITY
인하대병원

A3SECURITY

02

Business Area

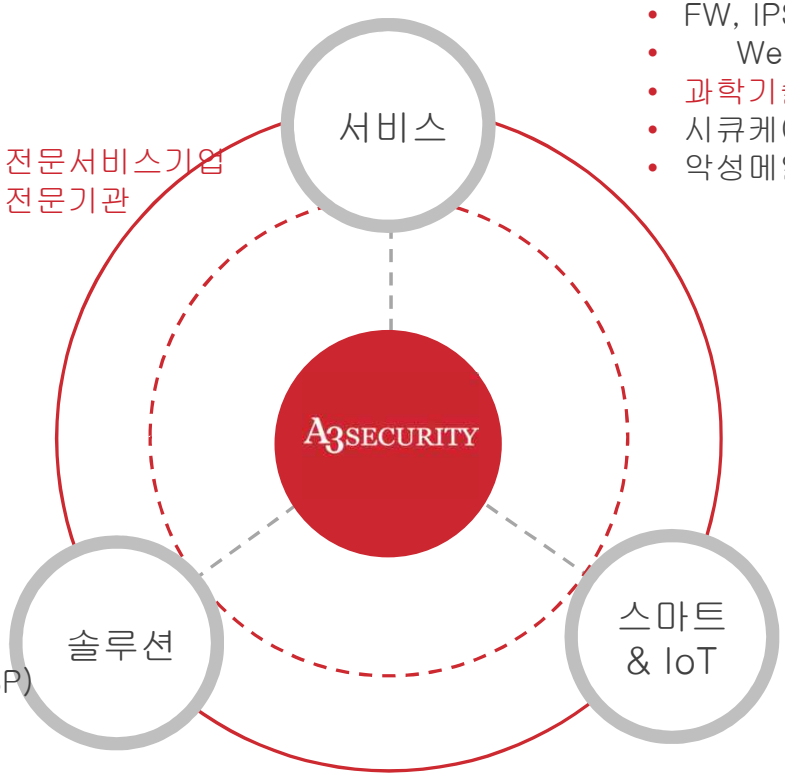
사업영역

› 사업 개요

We make your value secure!

정보보호서비스

- ISMS/PIMS/ISO27001 인증 컨설팅
- 주요정보통신 및 금융위 기반시설 컨설팅
- 개인정보보호 컨설팅
- 기술적 취약점 진단 컨설팅
- 모의해킹 및 소스코드 분석
- 개인정보 영향평가
- 과학기술정보통신부 지정 정보보호 전문서비스기업
- 행정안전부 지정 개인정보영향평가 전문기관



- 파견관제
- FW, IPS, WAF, DDoS, WIPS,
- Webshell 원격관제 및 장비임대
- 과학기술정보통신부 지정 보안관제 전문기업
- 시큐케어 서비스
- 악성메일 모의훈련 서비스 등 제공

정보보호통합솔루션

- 통합 정보보호 관리 시스템(Rfinder ESP)
- 감사시스템 등 개발 · 구축
- 보안SI 및 통합 유지보수

스마트 시스템 & IoT

- 무인주문결제시스템 (MENU BOX)
- DID (Digital Information Display)
- 듀얼망분리PC · 미니PC · 산업용PC 제작

A3SECURITY

03

Business Information

사업소개

> 보안컨설팅

보안관제

We make your value secure!

A3SECURITY 의 정보보호 컨설팅 서비스는 전산시스템, 네트워크, PC 등 IT 자산을 운영하고 관리하는데, 발생할 수 있는 모든 위험 요소에 걸쳐 세밀한 분석과 함께 체계적인 대책 수립을 제공합니다.

관리 · 물리 · 기술적 관점에서 가능한 모든 취약점들을 파악하고 위험 요소들을 분석하여 실질적이고 구체적인 보안대책을 수립합니다.

에이쓰리시큐리티는 기업 및 조직이 갖춰야 할 보안 모델로써 'A3Security Model'을 권고하고 있습니다.
이는 BSI의 ISO27001, ISACA의 COBIT, FFIEC 등의 보안모델들을 국내의 전산 관리 환경에 맞춰 개선시킨 새로운 정보보호 프로세스입니다.

A3 Security Model

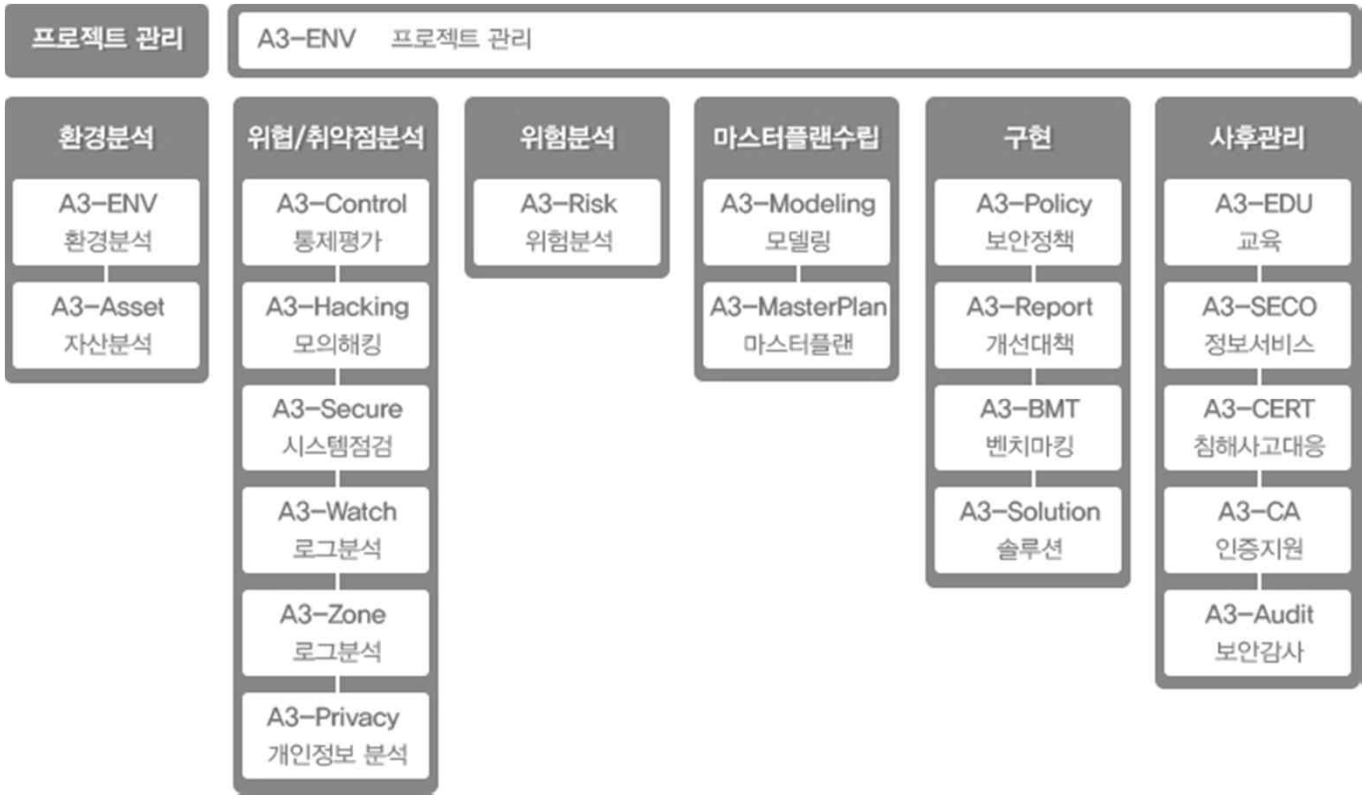
정보보호컨설팅 주요영역

- 정보보호 마스터플랜 컨설팅
- 주요 기반시설 취약점 진단
- ISMS/PIMS 인증 컨설팅
- 개인정보보호 컨설팅
- 보안감사
- 모의해킹 및 소스코드 진단 컨설팅
- 개인정보보호 컨설팅 및 개인정보영향평가

정보시스템 보안의 모든 영역에 걸쳐서 정책 제안, 대응 및 해결 방법은 물론, 최적의 기술지원과 예방대책을 제시함으로써 고객의 정보시스템 보안에 가장 적절한 해결방안을 제시합니다.
물리적 보안, 네트워크 보안, 로컬 시스템의 OS보안, 응용프로그램 보안 등 모든 계층에 걸쳐 각각의 세부적인 보안정책 수립 및 절차보안 구현, 보안감사를 통해 침해사고를 예방하고 대외적 신뢰도를 향상시킴으로써 기업 경쟁력을 강화시킵니다.

A3SECURITY 는 기업이 갖춰야 하는 보안 모델로써 A3Security Model을 권고하며, 이를 구현하기 위한 접근방법론으로써 TASCoM(The A3Security Consulting Methodology)을 자체 개발하여 보유하고 있습니다.
TASCoM은 정보보호컨설팅전문업체 선정 및 국내 보안컨설팅 최다 수행이라는 사실을 통해 그 체계성과 객관성, 전문성, 적합성 등을 공식적으로 인정 받고 있습니다.

TASCoM 세부모듈



TASCoM은 Best Practice와 Standard를 기반으로 A3Security가 개발한 보안 컨설팅 방법론입니다.
총 6 Steps, 20 Modules의 체계적인 아키텍처로 구성되어 있으며, 고객 환경에 맞춰 최적의 Modules을 조합하고 적용함으로써 최상의 결과를 도출합니다.

연간컨설팅(On-Going) 서비스는 기업과 조직의 정보보안 활동 수행을 위한 전문 인력 투입 등의 효과적인 지원과 구체적인 업무 수행방안을 제시하여, 정보보호 문화 정착과 정보보안수준 향상에 기여하기 위한 서비스입니다.

정기적인 취약점진단

• 취약점 분석을 통한 잠재적인 정보보안 위험 요소 제거, 정보보호 기준수립을 통한 정보보호
수준 향상 및 보안강화

모의해킹

• 내부 및 외부에 대한 전체적인 점검을 통해 정보유출 요소 제거, 신규 취약점 및 신규 장비들에 대한 점검을 통해 안전한 보안환경 제공

연간컨설팅 서비스를 통한
안전한 정보시스템 관리 및
정보보안 수준 향상

정보보호 자문

• 계획 수립 및 조직 구성 시 전문적인 자문을 통해
효율적인 보안시스템 도입 및 계획 수립 가능

정보보호 교육

• 임직원들의 생활보안 및 내부정보 유출에
대한 보안 인식강화, 교육을 통한 훈련으로
보안 대응능력 향상

조직의 보안체계가 효과 · 효율적으로 구현 · 운영되고 있는지를 문서체계 및 증빙자료, 실사 등을 통해 점검합니다. 보안관리체계가 마련되어 운영되고 있는 조직에서 현 관리체계 구성 및 운영의 적절성에 대한 검토를 하고자 할 때 적합한 서비스입니다.

방송통신위원회 취약점 분석 및 평가 기준을 반영한 보호대책을 수립합니다(정보통신기반보호법에 명시된 조항 준수). 관련 법에 따라 대상 기관・조직은 매년 취약점 분석 및 평가를 실시하여야 합니다.

금융감독위원회 취약점 분석 및 평가 기준을 반영한 보호대책을 수립합니다(전자금융감독규정에 명시된 조항 준수).
관련 법에 따라 대상 기관・조직은 매년 취약점 분석 및 평가를 실시하여야 합니다.

기술적 취약점 진단 컨설팅은 고객과 마주하는 웹을 시작으로 네트워크, 보안시스템, 서버, DB, 내부 사용자 PC까지 침해사고의 발생 가능성이 존재하는 취약점을 발견 및 조치하여, 침해사고의 발생 가능성을 낮추고, 향상된 보안 수준을 유지할 수 있도록 지원하는 서비스입니다.

기술적 취약점 진단 컨설팅

대 고객서비스 및 내부망 시스템

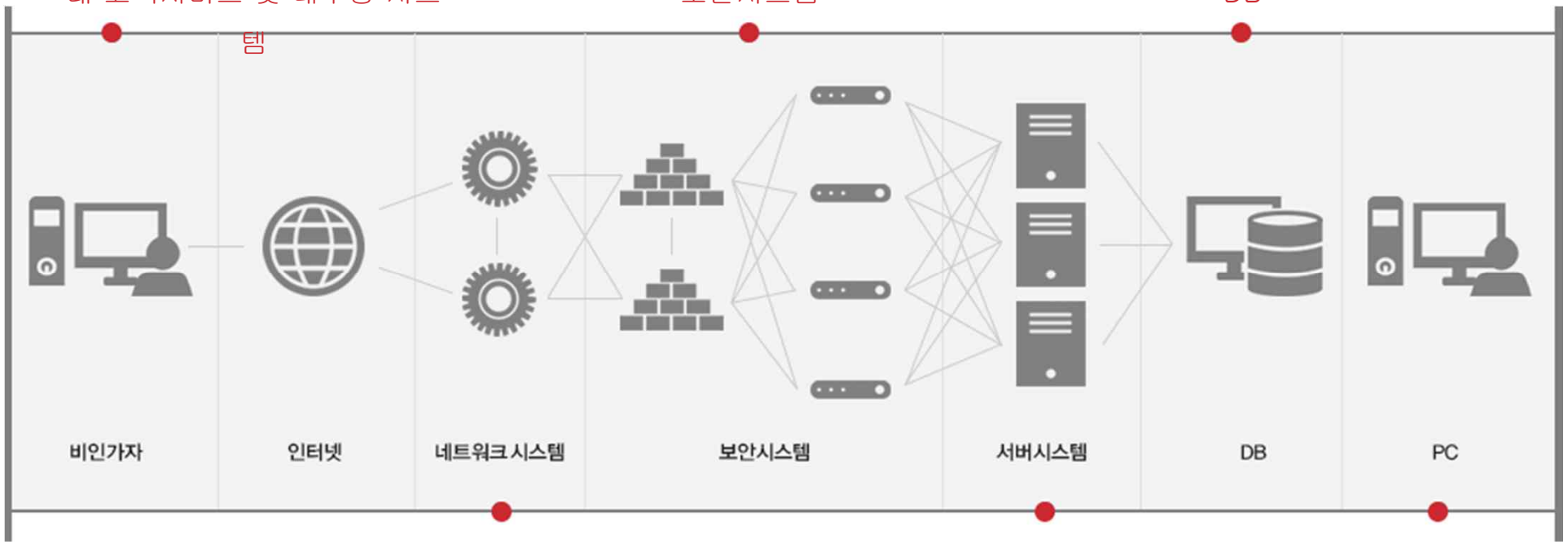
• OWASP Top 10 취약점 점검, 국정원 8대 취약점,
개인정보 노출가능성, 내/외부 시나리오 기반 점검

보안시스템

• 보안시스템 설정 점검, 보안시스템 구조적
문제점 점검, 보안 기능상 문제점 점검, 운영
관리상 문제점 점검

DB

• 사용자 작업에 대한 감사, DB계정 별 접근권한,
관리계정 접근제어, 백업/복구 정책의 적합성,
DB관련 파일시스템 접근제한



네트워크 시스템

• Config 설정오류 분석, 계정/패스워드
보안 상태, 접근제어 설정 점검

서버 시스템

• 사용자 관리상태 점검, 파일 시스템 점검,
서비스 관리 점검, 접근제어 점검, 로그 및
인증 현황 점검

PC

• 비인가자 접근제어 점검, 각종 주변장치
관리 점검, 보안패치 업데이트 점검,
백신 사용 실태 점검, 패스워드 설정 점검

기업 및 조직의 비즈니스 목적에 적합한 정보보호 관리체계를 구축, 유지, 관리하여 정보보호 수준을 제고하고, 한국인터넷진흥원이 관장하는 정보보호 관리 분야의 국내 표준인 ISMS-P인증 획득 및 갱신을 지원하는 서비스입니다.

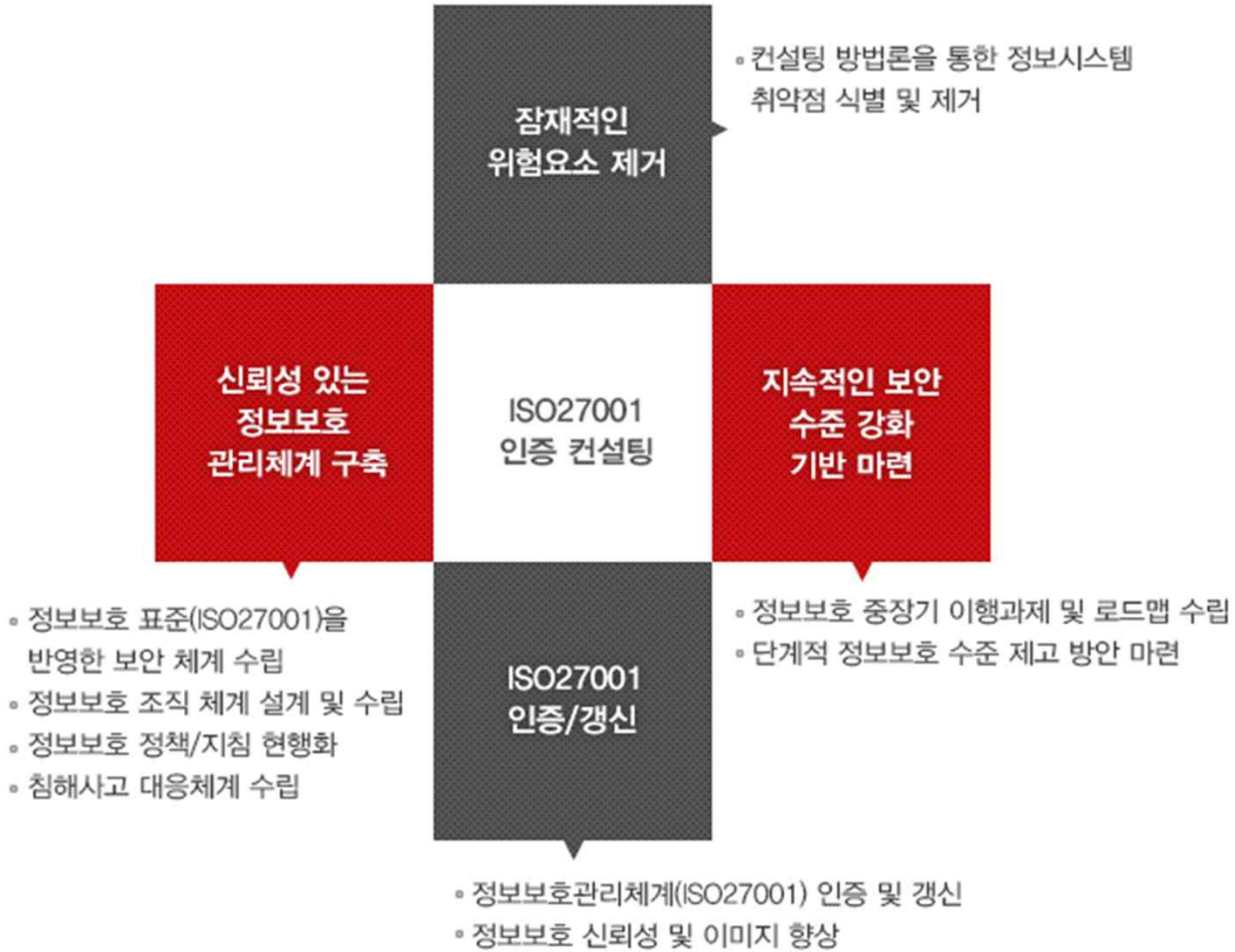
ISMS-P 인증 컨설팅

ISMS-P

(Personal Information & Information Security Management System)

기업 및 조직의 비즈니스 목적에 적합한 정보보호 관리체계를 구축, 유지, 관리하여 정보보호 수준을 제고하고, 유럽을 중심으로 전세계적으로 확산되고 있는 정보보호 관리 분야의 국제 표준인 ISO27001 인증 획득 및 갱신을 지원하는 서비스입니다.

ISO27001 인증 컨설팅



전 세계에 걸쳐 개인정보를 보호하기 위한 조치들이 각 국의 법과 제도에 추가되고 있습니다. 이에 따라 공공 부문과 민간 부문에
걸쳐 개인정보를 취급하는 조직은 개인정보보호정책을 수립하고, 개인정보보호책임자를 지정하며, 각종 기술 및 관리적 보호조치를 적용해야 합니다.

개인정보보호 컨설팅 방법론 구성

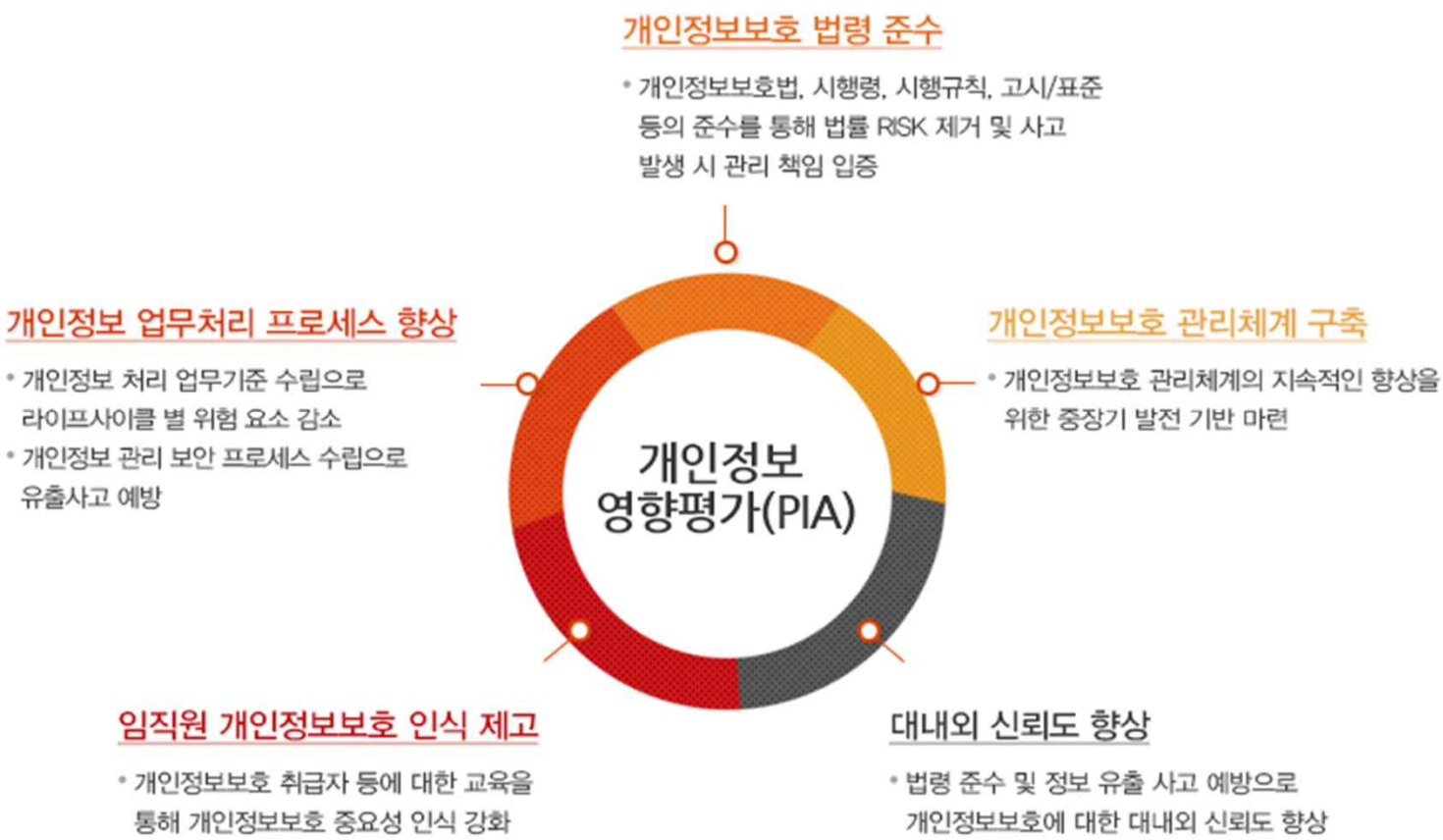
*주1) PI : Private Information *주2) PIP : Private Information Protection

에이쓰리시큐리티는 개인정보의 라이플 사이클에 걸쳐 개인정보를 취급하는 시스템과 취급 프로세스에 존재하는 위협과 취약점을 식별하고 위험을 평가하여 고객사에 적합한 보호대책을 수립하여 드립니다.

A3Security 개인정보보호 컨설팅 방법론은 국제 표준(ISO22307)에 부합하며, 공공 부문을 포함하여 주요 산업분야(유통, 통신, 금융, 교육, 의료 등)에 적용 가능한 방법론으로써 각 산업별로 요구되는 Legal Compliance와 개인정보보호 특성을 모두 고려하여 설계된 방법론입니다.

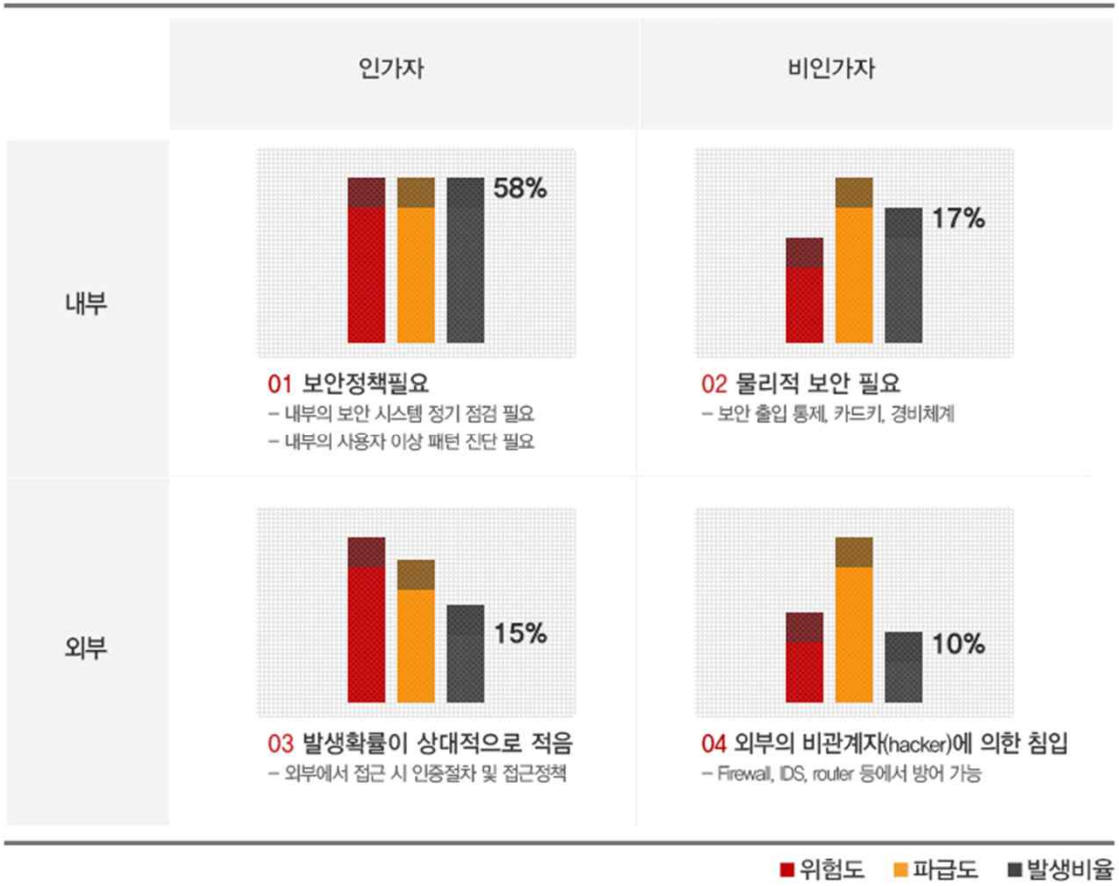
개인정보 보호법에 의거하여 일정 규모 이상의 개인정보 파일을구축·운용 또는 변경·연계하려는 공공기관은 해당 개인정보 파일 처리에 대한 영향 평가를 수행하여야 합니다. 개인정보 영향평가(PIA)는 전문 교육을 통해 인증 받은 인력을 통해서만 진행할 수 있으며, 에이쓰리시큐리티는 인증된 인력의 충분한 확보를 통해 높은 품질의 서비스를 제공합니다.

개인정보 영향평가 컨설팅



A3SECURITY 의 모의해킹 전문팀이 실제 공격자 관점으로 서비스의 주요 취약점을 도출하고 해결방안을 제시하는 서비스입니다. 다양한 IT 서비스 환경을 고려하여 각 정보시스템 유형별(웹, 네트워크, 서버, 전자우편, 사용자, PC, DBMS, 특정 어플리케이션 등) 시나리오를 세분화하여 진행합니다.

위험 요소에 따른 위협 유형 구분



웹 방화벽, 메일 보안 솔루션, 암호화 솔루션, PC 방화벽 등 각종 보안솔루션의 우회 가능성 점검에서 다양한 최근 IT인프라에 맞추어 3G, 4G 등의 모바일, WEB 2.0, VOIP, IPTV, 클라우드 서비스 등의 신기술에 이르기까지 서비스에 위해가 가지 않는 범위 내에서 다양한 해킹 기법을 통해 Critical한 보안 이슈를 도출하고 대책을 제시합니다.

A3SECURITY 의 소스코드 진단 컨설팅은 응용 프로그램 내에 보안의 잠재적 취약점을 발견하여 제거함으로써 안정적인 서비스 운영을 지원하는 컨설팅 서비스입니다. 해킹이 빈발하거나 안정성이 떨어지는 서비스, 운영으로 이관되지 않은 개발 및 변경된 서비스에 특히 효과적입니다.

어플리케이션 진단 서비스

- 진단 대상에 따라 일반 업무용 어플리케이션 진단과 웹 어플리케이션 진단으로 구분됩니다.

01.업무용 어플리케이션 진단

고객의 자체 개발된 응용시스템에 대해 모의해킹 and/or 소스코드 수준의 진단을 통해 취약점을 파악하고 보안대책을 수립하고 제시합니다.

02. 웹 어플리케이션 진단

고객사 제공 웹 서비스에 대하여 사용자 입력 체크, 인증지원, 접근 제어 등의 보안설정이 적합하게 적용되어 있는지 설계/구현상의 취약점을 점검하고, 각 언어(ASP, JSP 등) 상의 취약점을 상세하게 점검합니다.

- 어플리케이션 진단을 위한 각 단계는 크게"AS-IS Analysis", "To-Be Modelling"으로 구분하여 진행됩니다.

AS-IS Analysis

TO-BE Modelling

현황 분석 업무협의
- 보안진단 범위 협의
- 진행 일정 협의
- 사용된 언어 파악
- 취약점별 가중치 설정

설계/구현 상 취약점 점검
- 어플리케이션 기본분석
- 표준 점검항목 작성
- 커스텀 점검항목 작성
- 소스코드 점검

언어적 취약점 점검
- 자동화된 툴을 이용한 소스코드 점검
- 수동적 소스코드 점검

해결책 및 가이드라인 제시
- 결과보고서 작성
- 보안 프로그래밍 체크리스트 작성
- 보안 프로그래밍 가이드라인 작성

Application 보안 요소는 정보 자산을 중심으로 보안 요소 별 상관 관계를 도출 한 후, 보안 기능이 적절히 고려될 수 있도록 배치되어야 합니다.

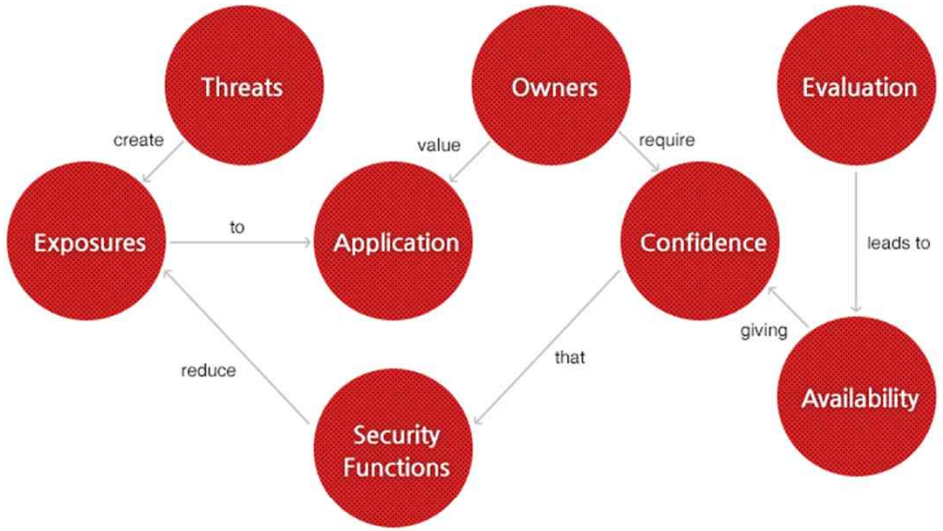
Application 보안 요소 및 관계

Security Policy
(보안 정책, 절차, 지침)

Best Practices
(Security Organization, Physical, Network, System, Application, OA, Operational Security 등)

Processes & Methods	Security Goals	Architecture
자산분석/취약점 분석	가용성	Security Infrastructure
위험 관리	인증/권한	네트워크
모니터링 & 보안 사고 관리	접근제어	시스템(서버)
보안 감사	기밀성	응용시스템
연속성 계획	무결성	PC/OA
	책임성	물리 환경적

Legal & Regulatory Environment



보완기능			
	Authentication	Authorization	Accounting
	Confidentiality	Integrity	Availability

A3SECURITY

03

Business Information

사업소개

보안컨설팅

보안관제

We make your value secure!

AEGIS
Advanced Event Guidance Information Service

A3-AEGIS(Advanced Event Guidance Information Service)관제서비스는 지속적으로 증가하는 보안 위협으로부터 고객의 정보자산 손실을 막기 위해 필요한 모든 시스템을 실시간으로 모니터링 하여 즉각적인 대응, 관리가 가능하도록 필요한 전문인력과 프로세스, 기술 및 전문지식을 제공하여 고객이 자신의 핵심역량에 집중할 수 있도록 하는 서비스입니다.

"전문 보안관제 서비스 필요" · 보안위협의 증가 ·

A3-AEGIS 관제서비스는 지속적으로 증가하는 보안위협으로부터 고객의 정보자산 손실을 막기 위해 필요한 모든 시스템을 실시간으로 모니터링하여 즉각적인 대응, 관리가 가능하도록 필요한 전문인력과 프로세스, 기술 및 전문지식을 제공하여 고객이 자신의 핵심 역량에 집중할 수 있도록 하는 서비스입니다.

대외적 요구

- 성장하는 신기술 대비 정보보호 기술 습득의 어려움 발생
- 침해 기술의 지속적인 발달
- 보안 위험성의 지속적인 증가
- 정보자산 침해시도 매년 증가
- 대응체계 수립 필요
- 대응역량 강화 필요

내부적 요구

- 보안장비의 유기적인 통합관리 및 대응체계 구축 필요

관리의 어려움 >
- 발생하는 이벤트의 분석을 위한 수집 및 분석 체계 미비
- 각 부서 / 지사
- 지속적으로 증가하는 보안 위협에 대응하기 위한 인력, 시간의 확대 필요

장애대응 부재 >
- 24 x 365 보안관제 시간 확대 필요
- 인력 및 전문 운영 기술 부재

고객사 정보시스템의 안정성 및 신뢰성 확보

신종 및 다양한 외부 공격의 효과적인 대응체계 구축	다양한 공격의 대응기술 공유로 관제능력 향상	보안취약점 점검을 통한 사이버 위협요소제거	모의해킹을 통한 정보시스템 안정성 향상	365 x 7 x 24 실시간 모니터링	정보 서비스 안정성 및 신뢰도 확보	침해사고 종합 예방 및 피해 최소화

AEGIS
Advanced Event Guidance Information Service

A3-AEGIS 서비스 도입 전 Cleaning Service를 진행하여 상주하고 있는 위험성을 사전에 제거하고, 서비스 도입 후 수행되는 Hardening Service를 통해 수준 높은 보안관제서비스를 제공하고 있습니다.

Cleaning Service

Hardening Service

기술 취약점 진

- 체크리스트, 보고서
- 대상 : 주요IT자산

정책 고도화

- 정보시스템 정책 고도화 권고
- 오탐율 감소, 효율 증가

웹 모의해킹

- OWASP TOP 10 기반
- 대상 : 서비스 중인 중요 URL

이력 관리

- 이력 관리
- 이슈 History 관리

이행점검

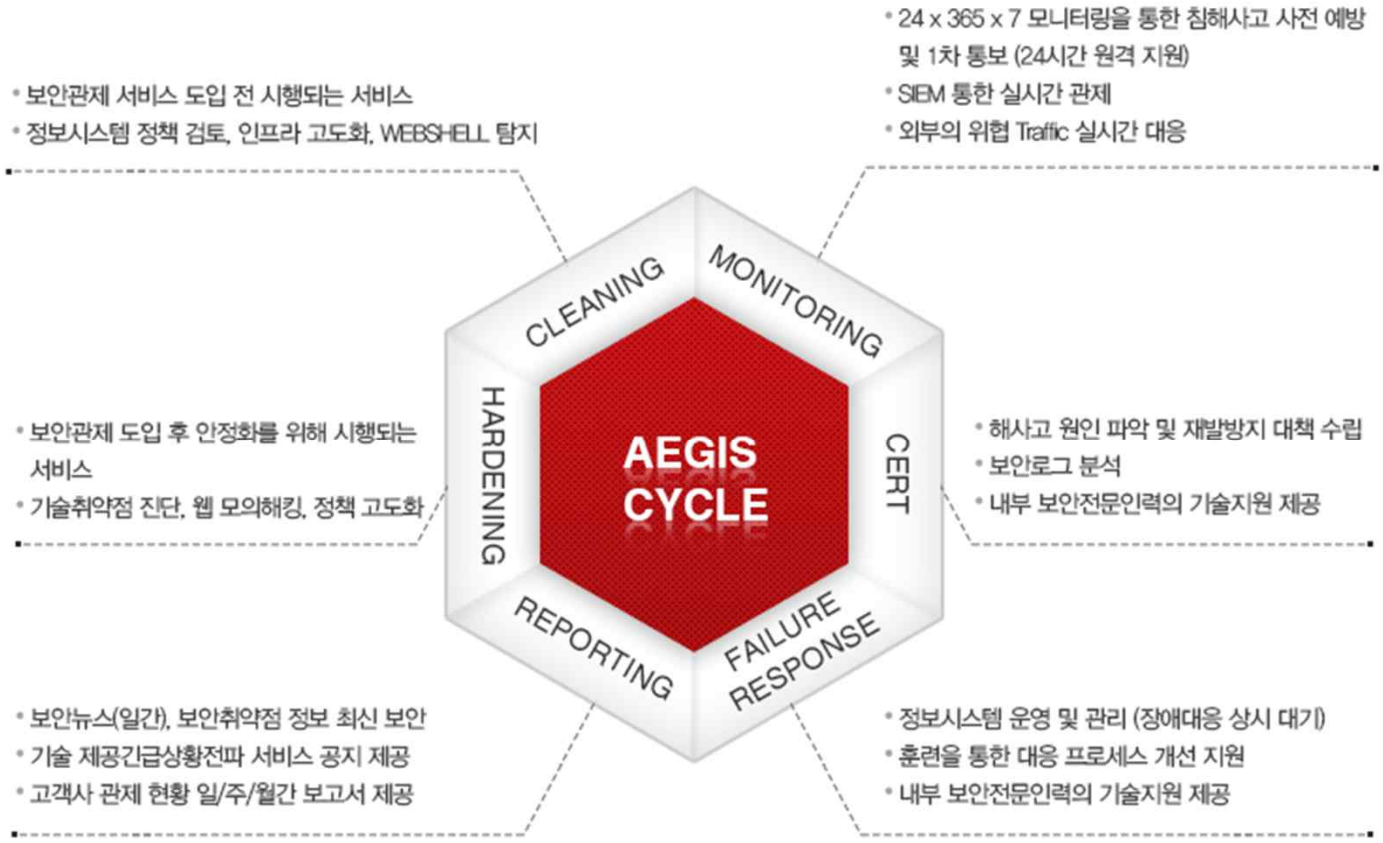
- 진단 및 정책 고도화 이행결과 확인

개선방안 제시

AEGIS
Advanced Event Guidance Information Service

A3-AEGIS 관제서비스는 SIEM 솔루션을 통해 에이전트 없이 로그를 수집, 저장하여 로그의 무결 성 보장 및 이벤트 상관분석을 수행, 최적화된 보안관리 서비스를 제공합니다.

AEGIS 사이클



A3SECURITY

AEGIS 서비스

AEGIS - Firewall

- 외부의 네트워크 보안 위협으로부터 실시간 차단 및 방어
- 방화벽 보안 정책의 실시간 관리 및 모니터링 대응

AEGIS - IPS

- 내/외부 침입행위에 대한 실시간 탐지 및 방지 서비스
- 보안 전문가에 의한 침입 이벤트 모니터링, 탐지, 침해대응 및 분석

AEGIS - WAF

- 내/외부 웹서버 위·변조 및 침해 실시간 탐지 및 대응 서비스
- 보호 대상 홈페이지 위·변조 검사, 차단, 분석 및 조치

AEGIS - Anti-DDos

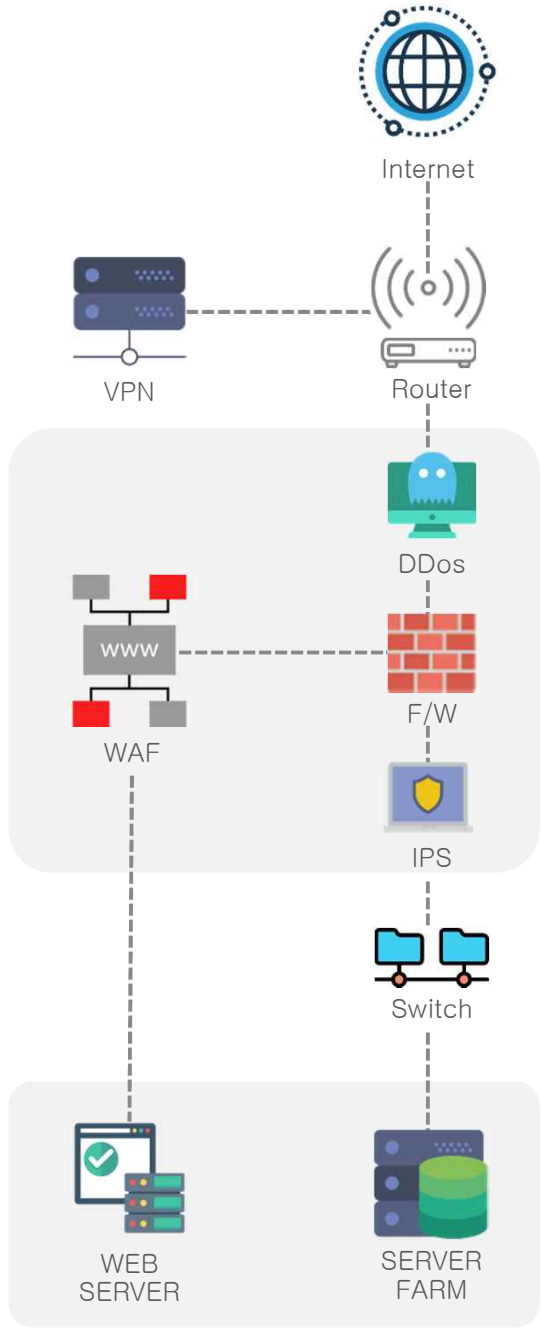
- DDoS 공격으로 부터 네트워크 서비스의 가용성 확보 서비스
- DDoS 실시간 감시로 네트워크 비즈니스 가용성 보장 및 대응

AEGIS - WIPS

- 무선랜 환경의 내·외부 위협에 대한 실시간 차단, 탐지 서비스
- 인가되지 않은 무선통신에 대한 탐지 및 차단을 통하여 고객의 내부자산 보호

AEGIS - Webshell

- 웹쉘 패턴 실시간 탐지 및 차단 통한 웹해킹 사전차단 서비스
- 웹쉡 업로드 위협으로부터 내부 기밀정보를 안전하게 보호하기 위한 서비스



A3SECURITY

감사합니다.

www.a3sc.co.kr

서울시 영등포구 당산로 171 금강펜테리움IT타워 702호
Tel. 02-6952-2511 | Fax. 02-6952-8661
e-mail. hello@a3sc.co.kr

We make your value secure!