Partner Webinar

Cisco Security Solution
CX Lifecycle Adoption & 서비스

Cisco Customer Experience (CX)

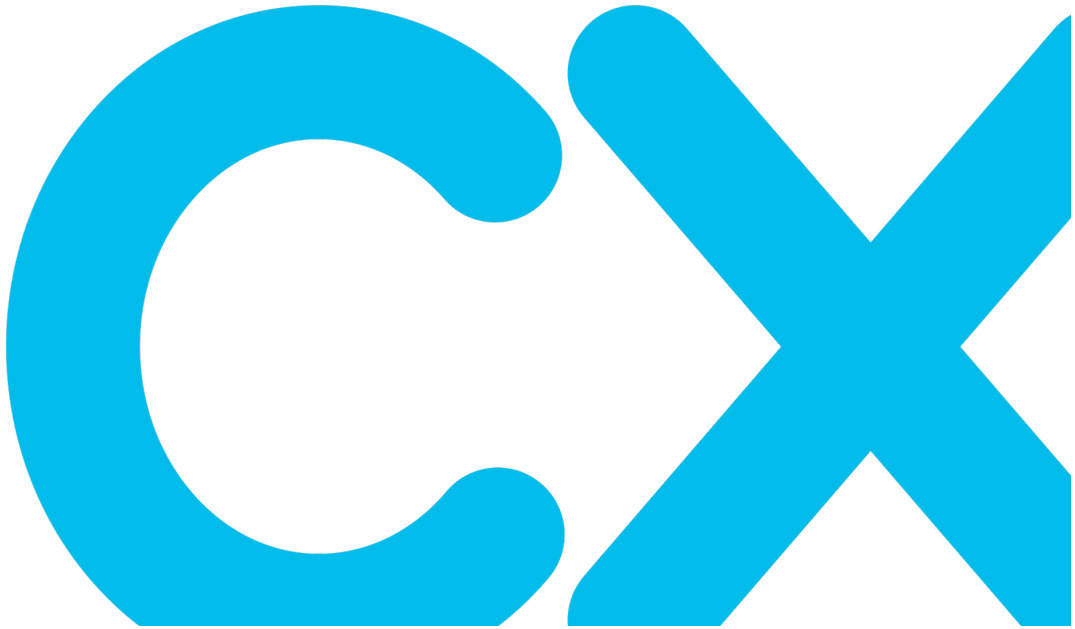
홍용수 상무, 신정섭 이사, 김종현 이사
Customer Experience
Cisco Systems Korea

2023년 6월 30일

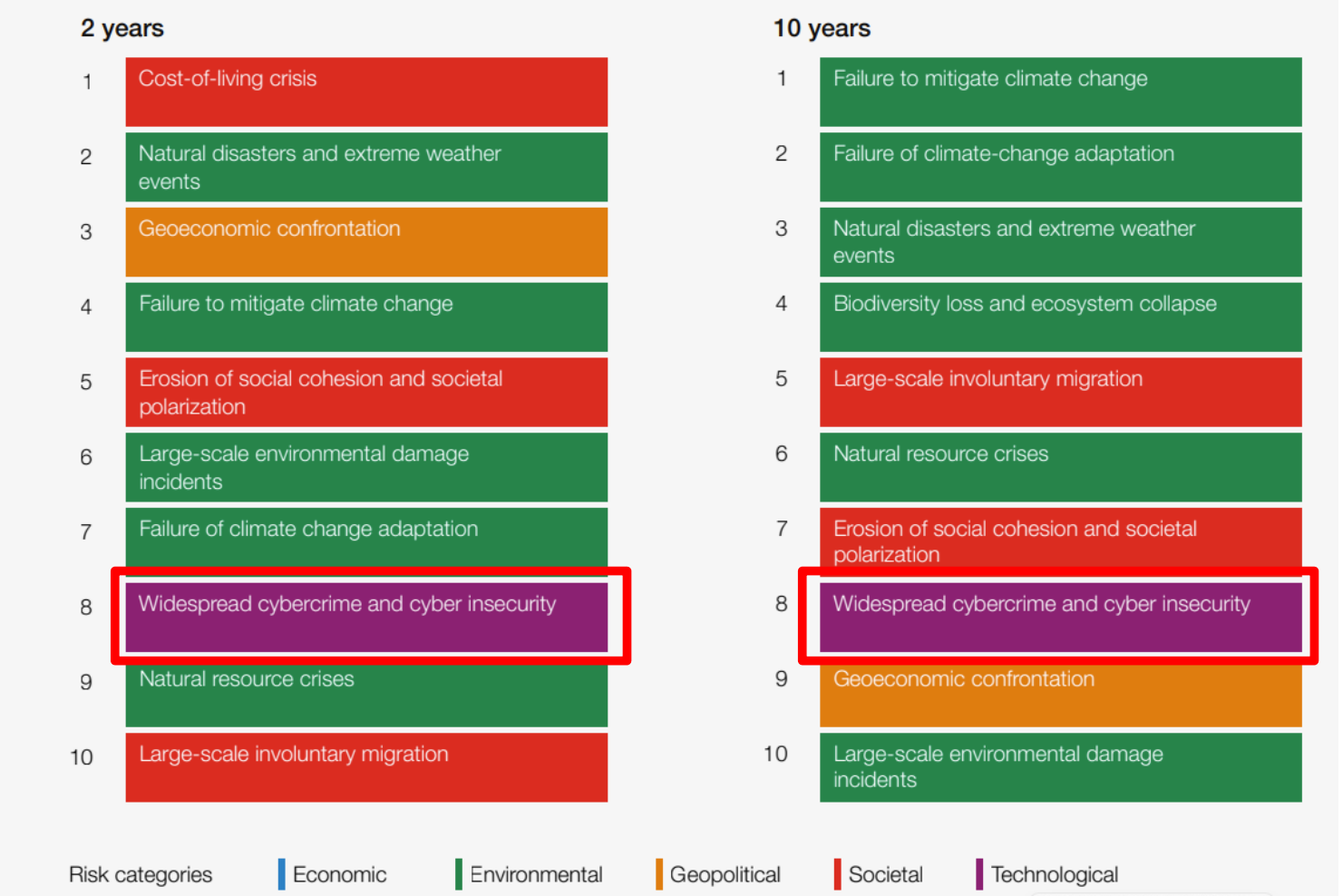
오늘의 주제

1. Why Cisco Security ? (다른 측면에서)
2. Lifecycle 기반의 CX Adoption 및 건강검진 프로그램 소개
3. 시스코 CX Security 서비스 포트폴리오와 사례

Why Cisco Security?



Key Global Risk : Cybersecurity



Source: World Economic Forum's Global Risks Report 2023

기업들의 세번째 가장 큰 우려 :Cyberattacks

Source: World Economic Forum's COVID-19 Risks Outlook

Gartner **Security Trends 2023**

기술적인 고려사항 〈 구성원의 경험/라이프사이클

CISCO SECURE

Security Reference Architecture / Portfolio

cisco.com/go/sra

v3.1

TALOS THREAT INTELLIGENCE

Actionable threat intelligence | Collective responses | Comprehensive visibility | Signal identification | Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Kenna | Secure Analytics | SecureX
Secure Client | Talos Incident Response

SERVICES

Custom threat research on demand | Implement and manage | Incident response retainer | Managed detection & response | Strategy & assessment

CAPABILITIES

Network detection & response | Device discovery & insights | Endpoint detection & response | Open API platform & 3rd party native integrations | Risk-based vulnerability management | Security analytics | Security orchestration, automation & response | Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User/Device Security

SASE/REMOTE WORKER: Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

Cloud managed | VPN | Posture | Telemetry/ Visibility | Endpoint detection & response | DNS-layer security | Secure Web | Anti-virus/ Anti-malware | Query | Host FW | Mobile device management

Risk-based MFA | Passwordless | Device trust | Continuous trust

Email, Phishing, SPAM, BEC, DLP, content filtering | Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge
Duo | Secure Connect | Umbrella

Browser access control | Cloud access security broker | Cloud malware detection | Data loss prevention | DNS-layer security

Identity/ posture | FWaaS | RAaaS | Remote browser isolation | Secure web gateway

Tenant restrictions | TLS decryption | Zero Trust Network Access

On-Premises Network

SASE/SDWAN
Meraki | Secure Firewall
ThousandEyes | Viptela

Analytics | Application performance optimization | Cloud based orchestration | Cloud OnRamp

Digital experience monitoring | IPSec VPN | Integrated security | Middle mile optimization

Segmentation | Visibility | Group tag propagation

In the Office/Managed Location
Catalyst | DNAC | ISE | Meraki | Secure Firewall
Secure Network Analytics | Web Appliance

Application network gateway | Configuration orchestration | Content filtering | Encrypted visibility | Group tag classification

Identity/ pxGrid Cloud | Network access control | Network security analytics | NGFW | NGIPS

Security analytics & logging | Segmentation | Threat mitigation | Profiling

Industrial Threat Defense
DNAC | CyberVision | Industrial Networking
ISE | Secure Firewall | Secure Network Analytics

Anomaly detection | Compliance | Group tag classification | Identity/ pxGrid

Ruggedized | Segmentation | Threat mitigation | Visibility

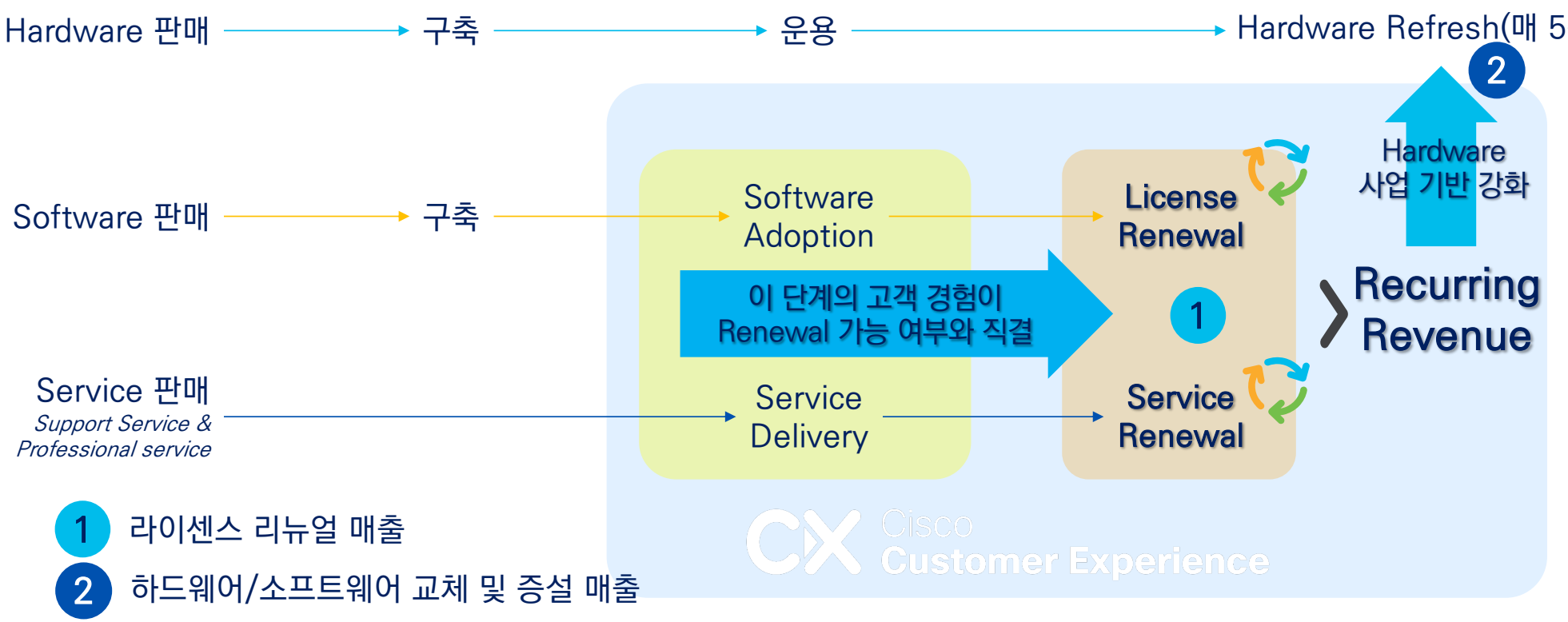
Workload, Application, and Data Security

HYBRID MULTI-CLOUD: ACI | Cloud Insights | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Secure Cloud Analytics | Secure Workload

Anti-virus/ Anti-malware | API security | App discovery | Cloud analytics | Cloud Native Security | Cloud Posture Management | DDoS, WAF/Bot | Identity/ pxGrid | Micro/Macro Segmentation | Run-time application | Telemetry | Threat mitigation | Visibility

Security Solutions : Software License 기반..(Recurring Revenue)

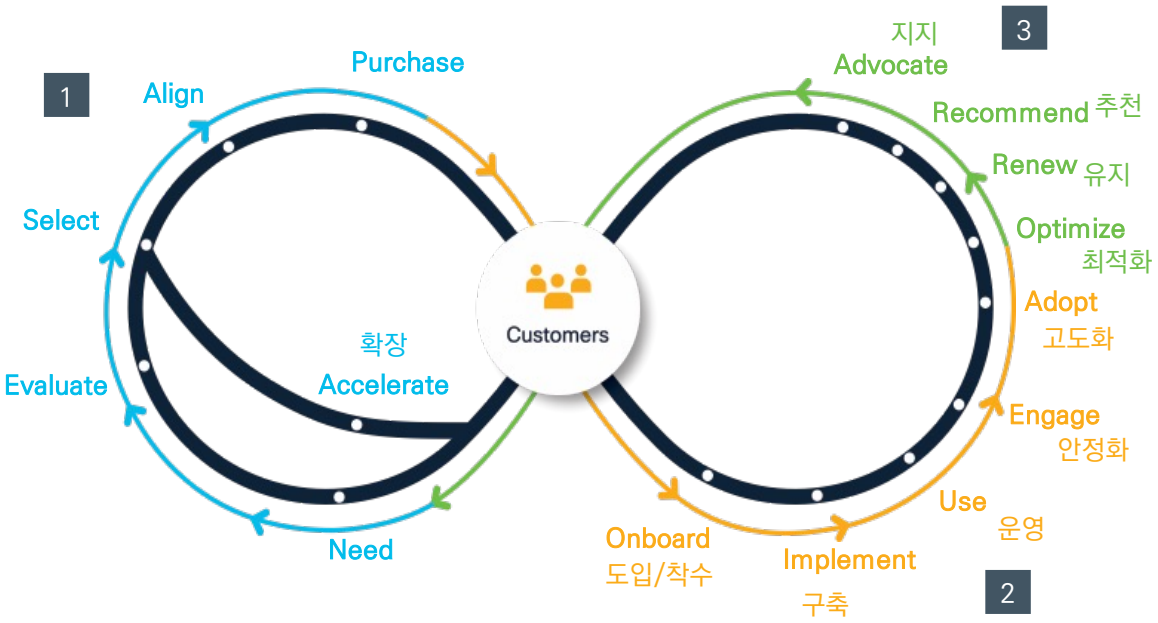
HW Price < SW License Price



1 라이센스 리뉴얼 매출

2 하드웨어/소프트웨어 교체 및 증설 매출

Recurring Software : 고객 Lifecycle 에 따른 Adoption이 중요



1 Strategic roadmap development	• 기술전략로드맵 개발 • 고객의 비즈니스 결과를 위해 가장 적합한 기술 솔루션 정의
2 Learning, implementation and adoption	• 기술력과 학습 맵을 통해 고객이 적시에 적절한 정보 취득 가능 • 솔루션의 단계별 구현 및 활용 • Lifecycle Adoption 진행
3 Continuous optimization and innovation	• 지속적인 최적화 및 업그레이드 • 툴과 원격관리를 통한 통찰력과 아이디어의 지속적인 제공

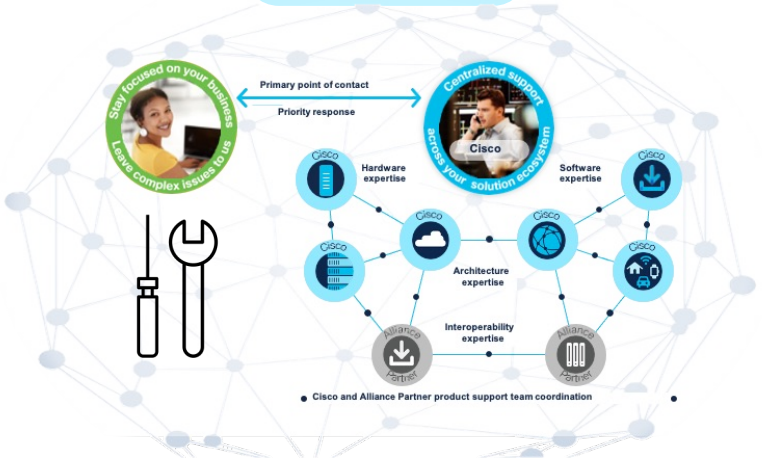
시스코 Customer Experience (CX) 의 지원 체계와 서비스

Cisco Customer Experience

60 + 18

Support Service

TAC & Expert Care

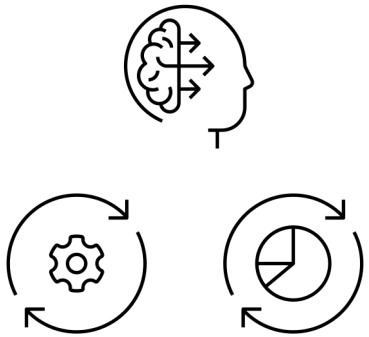


20 +

Professional Service

Consulting, Advisory & PDI*

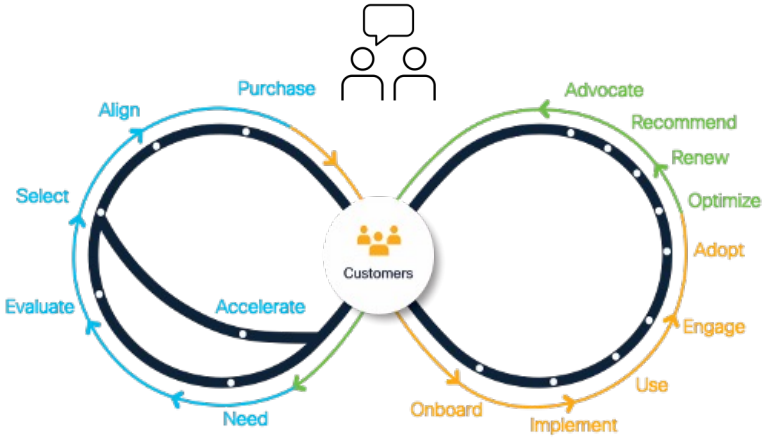
*Plan, Design & Implementation



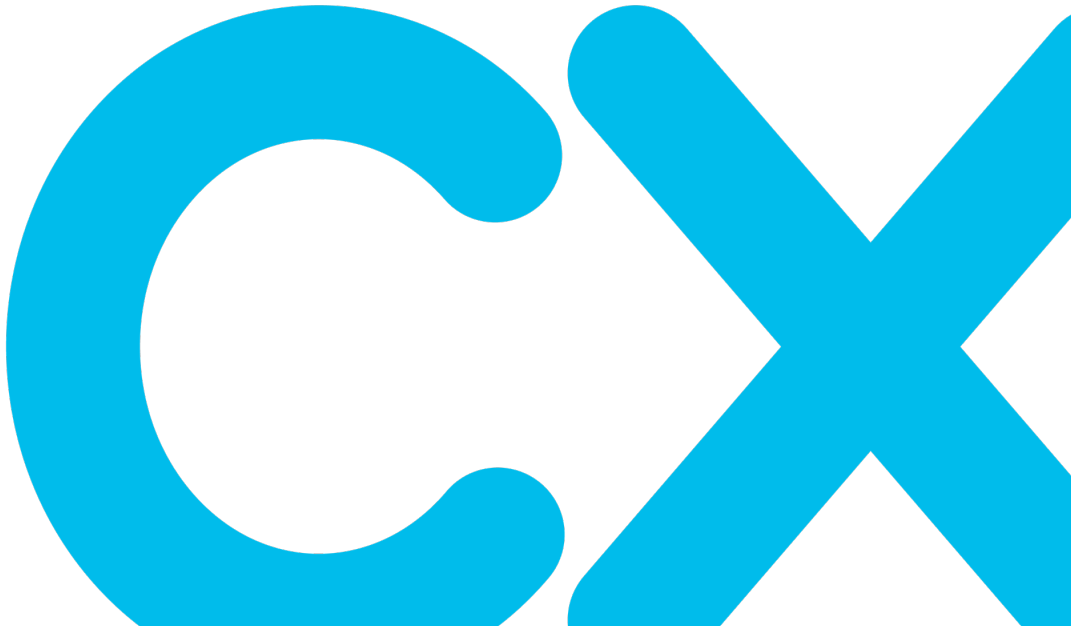
28

Customer Success

Solution Adoption Journey



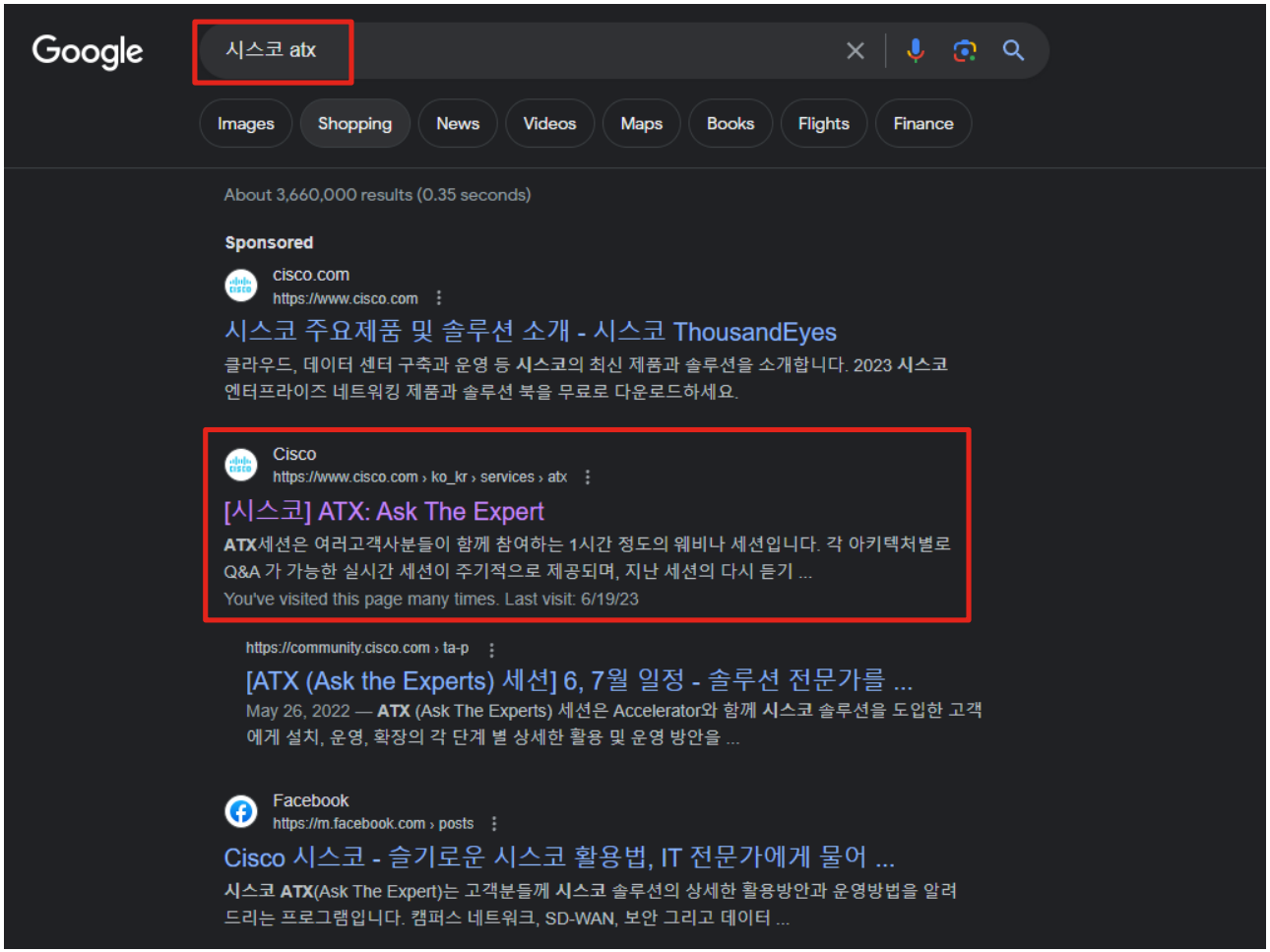
Lifecycle 기반의 CX Adoption 및 건강검진 프로그램 소개



ATX(Ask The Experts) 란?

- 일-대-다 대화식의 시스코 전문가와 함께하는 웨비나 세션입니다.
- 기술 Adoption 에 대한 어려움이나, 다양한 기술에 관심이 있는 고객분들과 파트너가 참여 할 수 있습니다.
- 기술관련 질문사항을 시스코 전문 엔지니어를 통해 실시간 답변 받으실 수 있습니다.(웹엑스 채팅/이메일)
- 주1회 금요일 오후2시(Security)부터 1시간~1시간30분 동안 시스코 웹엑스로 진행합니다.

ATX(Ask The Experts) 시작하기



ATX(Ask The Experts) 등록하기

ACC(Accelerator) 란?

- 일-대-일 대화식의 오프라인/온라인 세션입니다.
- 고객을 대상으로 소규모 그룹 단위를 위한 코칭 세션입니다.
- 디스커버리 미팅을 통해 Agenda 를 선정하고, 고객에게 필요한 주요 컨텐츠를 다루고 있습니다.
- 설계, 구축 및 운영 등 고객 현안 과제에 많은 도움을 드릴 수 있는 장점이 있습니다.
- 고객 요구사항을 청취하여 세션을 준비하며, 파트너사 담당자도 참여 가능합니다.
- 세션별 2~3시간 동안 3~4회 세션으로 진행 됩니다.

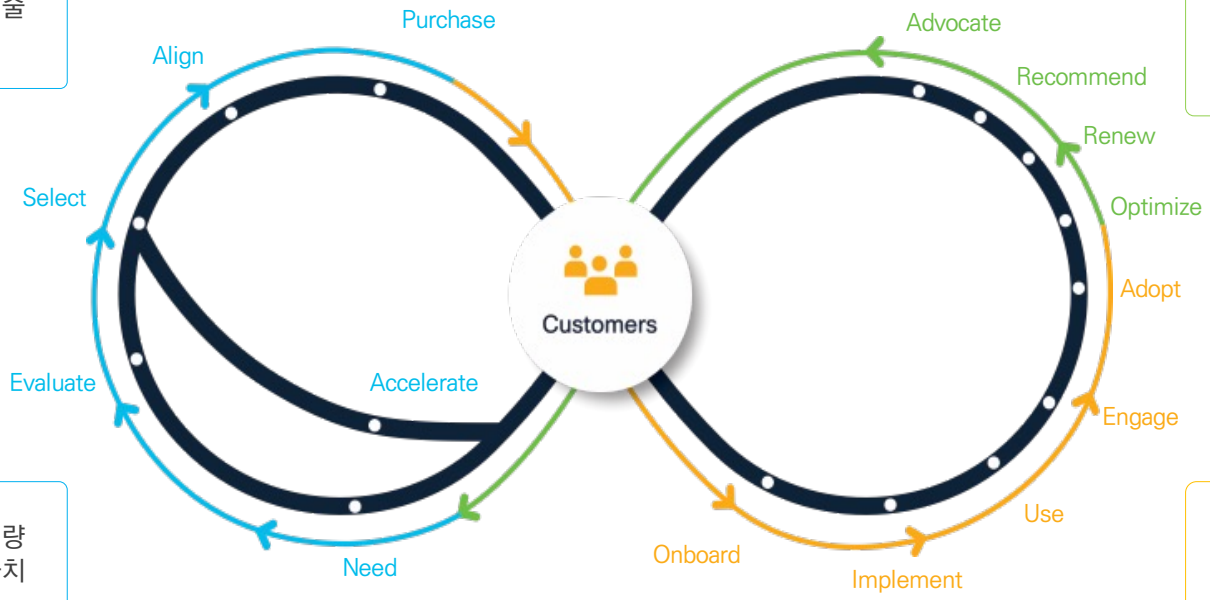
ACC(Accelerator) 장점은 무엇인가요?

- 라이프 사이클

  도입 – 구축 – 운영 – 고도화 – 내재화 – 최적화

단계별 과정

시스코 라이프 사이클 단계별로 기술 커리큘럼 제공



솔루션의 활용성 향상

ACC 세션을 통해 고객사에서 사용중인 혹은 도입 예정인 솔루션의 다양한 기능을 적용하여 활용성 향상

솔루션의 효율성과 가치 상승

솔루션 도입 단계부터 고객 기술역량 강화를 통해 솔루션의 효율성과 가치 상승

장애예방 및 안정성 향상

CX 라이프 사이클 단계 중 Health Check 프로그램을 통해 운영중인 시스템의 하드웨어 이상유무를 판단하고, 장애를 사전에 예방하는 안정성 향상

Health Check 소개

제공 솔루션
- Secure Firewall
- ISE

요구조건
- Secure Firewall
  - ✓ 소프트웨어 버전 : FMC & FTD Ver 6.0 이상
  - ✓ 하드웨어 : FirePower 2100, 4100, 9300
- ISE
  - ✓ 소프트웨어 버전 : 2.3 이상

기간
- 분석 기간 : 2주 ~ 3주

분석 범위
- 하드웨어 이상유무 분석(CPU, Memory, Disk 등.)
- 소프트웨어 버전 및 운용상태 점검
- 운용중인 Policy(Access Control Policy, Intrusion Policy 등)

수행 방법
- 1차 전문 분석 툴을 이용하여 현재 사용현황에 대한 세부적인 분석 후 전문 CSS 엔지니어를 통해 2차 결과 보고서를 작성 그리고, 결과 보고서 미팅을 통해 운영 환경 개선을 위한 모범 가이드 제공

산출물
- 1차 전문 분석 툴을 이용한 자동 분석 레포트(영문)
- CSS 엔지니어를 통해 1차 분석 레포트를 가공한 2차 결과 보고서
- 결과 보고서에 따라 추가 조치가 필요할 수 있음(TAC Case 및 AS)

Health Check 를 통한 Adoption 주요사례

Health Check 소개 및 진행여부 논의 → Health Check 결과보고서 미팅 → Accelerator 제안 및 아젠다/일정 협의 → 3~4회 Accelerator 진행을 통해 고객사 환경 최적화

성공적인 Adoption과 고객 기술 이해도 향상

- 은행 계열사 IPS Health Check 및 Accelerator 진행(IPS 기능 및 Snort 등)
- 금융 공기업 IPS Health Check 및 Accelerator 진행(IPS 튜닝 및 Snort 2,3 비교 등)

- Display 제조사 SNA Accelerator 진행
- 조선/선박 제조사 SNA Accelerator 진행
- 반도체 제조사 IPS Health Check 및 Accelerator 진행
- 대형SI 기업 ISE Health Check 및 Accelerator 진행

Health Check 결과보고서 샘플

IPS Health Check

Health Check 결과 및 Best Practice

하드웨어 및 구성

Health Check 전문 진단 프로그램을 통해 각 장비의 로그를 분석하여, 하드웨어의 이상유무와 조치방안에 대해서 제공 합니다.

Best Practice

현황 내용

- FMC & FTD :
  - + Health Check 진단 프로그램을 통해 분석된 하드웨어 상태 정보는 정상임을 확인 하였습니다.

권고 사항

- 하드웨어의 이상증상을 발견하였을 경우, 케이스 오픈하여 TAC 으로부터, 신속한 가이드라인을 받고 이슈를 해결 하시는 것을 권고 드립니다.

Platform Review

Devices	Severity	Description
	0 - Healthy	Critical Issue needs attention

Health Check 결과 및 Best Practice

Prefilter Policy

신뢰 할 수 있는 내부 통신 트래픽의 경우 장비의 성능향상과 최적화를 위해 Snort Engine 프로세싱 없이 Lina Engine(ASA) 에서 처리하는 기능을 제공 합니다.

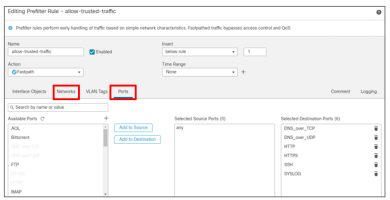
Best Pr

현황 내용

- Prefilter Policy 현황 :
  - + IPS 를 통과하는 트래픽 중 신뢰할 수 있는 traffic 을 분석하여 prefilter policy 를 설정하여 사용 중입니다.
- Prefilter Policy 장점 :
  - + 불필요한 Snort 프로세싱을 예외처리 함으로써 Snort Engine 을 Bypass 하는 EAC(Early Access Control) 를 사용하게 되어, Fast Path 프로세스로 디바이스의 성능을 최적할 수 있습니다.
  - + Tunnel 트래픽을 처리할 때 추가적인 유연성을 제공합니다.
    - GRE
    - IP-in-IP
    - Point-to-Point Protocol (PPTP)
    - Teredo port 3544

권고 사항

- Prefilter Policy 는 지속적인 관리가 필요한 Policy
  Secure Firewall 의 운영/관리 측면에서 신뢰할 수 있는 내부 혹은 외부 트래픽의 정보(Network, Port)를 수시로 업데이트 하여 IPS 의 성능을 최적하는 하는데 목적이 있습니다.



ISE Health Check

Health Check 결과 및 Best Practice

Platform Review

Health Check 전문 진단 프로그램을 통해 각 장비의 로그를 분석하여, 하드웨어의 이상유무와 조치방안에 대해서 제공 합니다.

Best Practice

현황 내용

- CPU & Memory 사용률 :
  - + Health Check 전문 분석 툴의 분석결과, 정상적으로 동작함을 확인
- 성능 관련 설정 부분 :
  - + Suppress repeated successful authentication options :
    - ➔ Disabled
  - + Logging Suppression Feature options :
    - ➔ Disabled

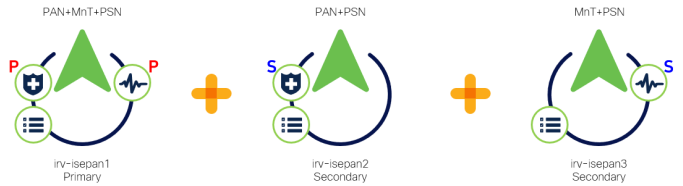
권고 사항

- CPU & Memory 사용률 :
  - + N/A
- 성능 관련 설정 미적용 부분 :
  - + Suppress repeated successful authentication options :
    - ☑ Enable
  - + Logging Suppression Feature options :
    - ☑ Enable

Health Check 진행요약

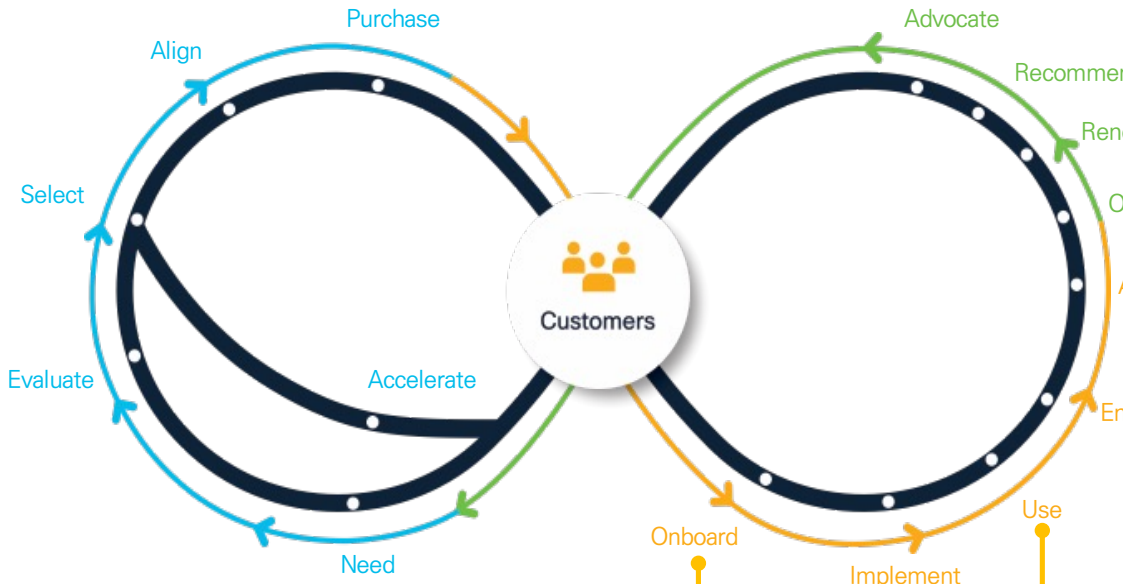
운영 디자인 현황

- PAN(Policy administration node)
  - + 모든 ISE 노드에 대한 Admin 역할
  - + 설정 변경 및 설정의 전반적인 부분에 대한 copy 제공
- MnT(Monitoring and troubleshooting node)
  - + 레포팅과 로깅 담당 node
  - + ISE nodes 로 부터 syslog 수집
- PSN(Policy services node)
  - + 정책 설정 node
  - + RADIUS/TACACS + Servers
- pxGrid controller
  - + Context-sensitive 정보를 공유



Health Check 이후 단계

Lifecycle Security Accelerator 컨텐츠 샘플



- Upgrade Planning and Best Practices: Upgrading Cisco Secure Firewall Techniques and Scenarios

- Use Case Health Check: Cisco Secure Firewall

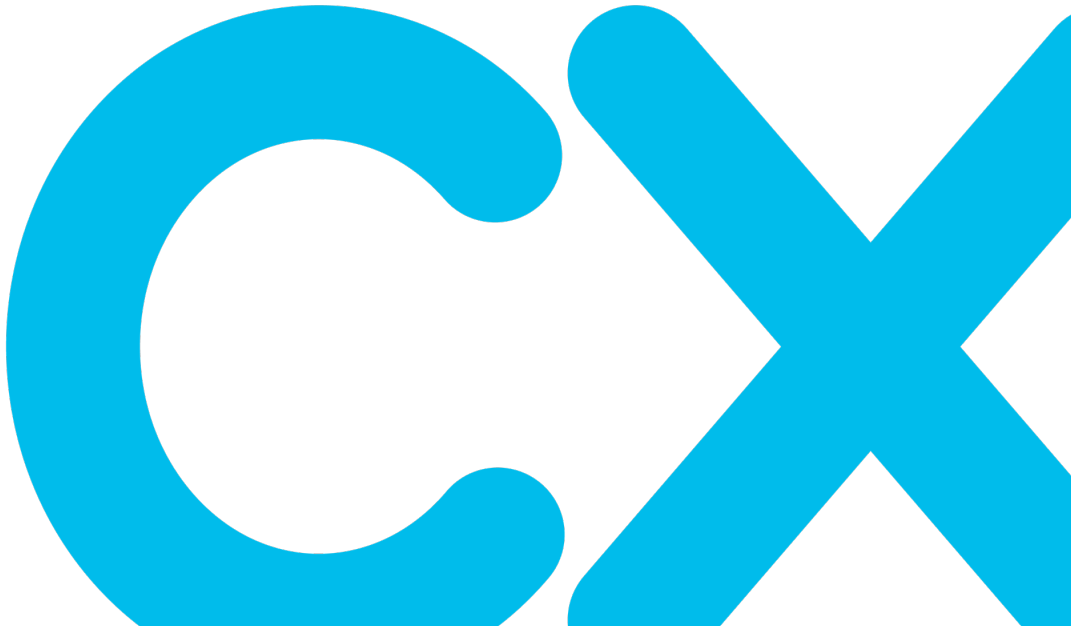
- Advanced Feature Deep Dive: TLS/SSL Decryption

- Feature Deep Dive: Advanced Malware Protection
- Feature Deep Dive: Intrusion Prevention System
- Feature Deep Dive: Network Discovery Deep Dive

- Deployment Best Practices: Access Policy Implementation Guidance
- Deployment Best Practices: Deployment Plan for the Internet Edge Firewall
- Migration Strategies and Best Practices: End-to-End Migration Strategy

- Architecture Transformation Planning: Design Guidance and Best Practices
- Getting Started: Firewall Management Center Essentials

Cisco CX Security 포트폴리오와 사례



전략 및 아키텍처에 중점을 둔 Advisory Services

주요결과

- **방향성, 구조, 명확성** – 잘 계획된 전략은 조직의 기술 및 보안 상태에 대한 명확한 방향과 구조를 제공합니다. 현재 상태와 목표 상태의 명확성을 높이는 것은 조직의 비즈니스 성과를 지원하는데 매 우 중요합니다..
- **투자 보호** – 전략 및 아키텍쳐 Advisor 서비스는 일반적으로 제품에 구애받지 않는 서비스로 기존 기술 투자를 확보하여 제안된 아키텍처에 재사용할수 있습니다.
- **위험 감소 및 보안 복원력 향상** – 조직의 보안 전략 및 아키텍쳐에서 기존의 격차와 약점을 인식하고 이를 해소하면 전반적인 위험 감소화 보안 복원력 향상에 도움이 됩니다.
- **보안 태세 강화** – 잘 설계된 네트워크 및 보안아키텍처는 견고한 보안 태세를 위한 토대를 제공하며, 전용 보안 제품 및 솔루션으로 이를 보완합니다..
- **규정 준수 및 감사 요건 용이** – 적절한 전략과 아키텍처를 갖추면 규제 및 규정 준수 요건이 용이해지고 감사 활동의 효율성이 높아 집니다.

Security Advisory Model

보안 아키텍처를 강화하기 위한 전문 지식

보안 프로그램 및 설계 개발

Cisco 보안 전문가의 전문가 조언을 받아 장기적인 전략 계획에 따라 보안 로드맵을 작성합니다

제로 트러스트 전략 서비스

정보 보안의 제로 트러스트 전략적 아키텍처 모델은 데이터, 네트워크, 사람, 워크로드 및 장치에 대한 신뢰를 구축하는 전략입니다

SOC 자문 서비스 (SOC Advisor Service)

평가 및 프로그램 설계 외에도, 귀사의 SOC(Security Operations Center) 개발 및 운영을 위한 세부 계획 수립을 지원합니다

보안 진단 (Security Assessments)

보안 진단(Security assessments): 사용자의 상태를 식별하고 개선을 위한 권장 사항을 제공함. 두 가지 유형:
전략적(Strategic): 컴플라이언스 및 리스크와 같은 주제에 대한 공급업체에 구애 받지 않는 진단 (Vendor-agnostic assessments)
전술적(Tactical): 애플리케이션 및 네트워크 아키텍처와 같은 비즈니스 크리티컬 솔루션에 대한 기술 중심의 토픽

사이버 보안 성숙도 프로그램 진단 Cybersecurity Maturity Program Assessment (CMPA)

보안 자문 서비스인 CMPA는 고객이 전반적인 보안 프로그램, 정책, 표준, 절차, 개별 보안 제어 및 리스크의 성숙도를 진단 평가할 수 있도록 지원합니다.

제로 트러스트 전략 서비스

(Zero Trust Strategy Service)

. 조직의 맥락에서 제로 트러스트 비전 설정
. 기존 기능을 보다 효과적으로 활용할 수 있는 기능과 변경이 필요한 위치 파악

. 제로 트러스트 니즈 분석
. 제로 트러스트 전략 로드맵
. 임원 요약/핵심 요약서

. 명확성과 목적을 가지고 제로 트러스트 전환 시작
. 제로 트러스트와 주요 혁신에 대한 시스코의 경험이 귀사의 성공을 견인할 것입니다

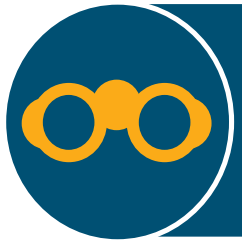
Services

. 제로 트러스트 전략 서비스

(Zero Trust Strategy Service)

SOC **자문 서비스**

(Security Operation Center Advisory Services)



How?

- ITIL®-based, informed by Cisco Talos™
- 비즈니스 및 기술 목표 조정
- 프로세스 및 오너쉽 결정

Deliverables

- 전략 및 요구 사항
- 디자인
- 활용 사례 및 계획

Why?

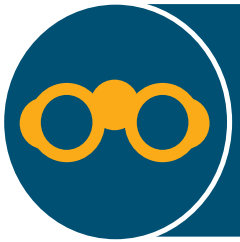
- 특정 상황에 적합한 Cisco 지적 자본
- 위험 감소 및 보안 상태 개선

Services

- 진단 (Assessment)
- 거버넌스 및 조직 디자인
- 비즈니스 케이스 개발
- 전략 및 분석
- 유스케이스 개발
- 솔루션 개발
- 구현 계획 개발
- 구현 후 지원

보안 진단 – 전략적

Security Assessments – Strategic



How?

- 보안 전문가의 인사이트 제공
- 최첨단 도구 및 프로세스 활용

Deliverables

- 상세 니즈 분석
- 권장사항 적용

Why?

- 보안 상태에 대한 명확한 뷰
- 캡이 어디에 있는 지 파악
- 위험을 줄이기 위한 권장 단계 파악

Services

- NIST Cybersecurity Framework
- 위험 진단

(Risk Assessment)

- 타사 위험 진단

(Third party Risk Assessment)

- 컴플라이언스 진단 (Compliance Assessment)
  - HIPPA and HITECH Assessment
  - ISO 27001/27002 Assessment
  - PCI-DSS Readiness Assessment

보안 진단 – 기술적

Security Assessments – Technical

- 보안 전문가 인사이트 제공
- 최첨단 도구 및 프로세스 활용

- 격차(gap) 및 권장 해결책에 대한 세부적인 결과서

- 보안 상태에 대한 명확한 뷰
- 격차(gap) 식별
- 권장 사항 적용 계획

Services

- 레드 팀 (Red Team)
- 네트워크 아키텍처 진단
- Penetration Test
  - Network
  - Wireless
  - Physical
  - IoT Devices
- Blackbox Web Application Assessment
- Application Security Architecture Assessment

사이버 보안 성숙도 프로그램 진단

Cybersecurity Maturity Program Assessment (CMPA)

- CMPA는 업계 모범 사례 및 국제 표준에 부합하는 인력, 프로세스 및 기술에 초점을 맞춘 포괄적인 사이버 보안 관리 프레임워크 를 사용하여 광범위한 평가를 제공

- 임원 및 관리자 요약 보고서
- 집중 영역별 세부 결과, 분석 및 권장 사항
- 보안 전략 로드맵

- 보안 상태에 대한 명확한 뷰
- 보안 프로그램 격차(gap) 식별
- 보안 프로그램 권장 사항

Services

- 성숙도 진단 (Maturity Assessment)
- Detail analysis
- Program Maturity Summary
- High-Level Security Strategy Roadmap
- 비즈니스 추진 요인에 맞춰 사이버 보안 성숙도 프로그램 및 기본 제어 기능을 개선하기 위한 지침 제공

Security Services

구축 서비스

- CISCO는 기술 및 네트워크의 여러 영역에 걸쳐 통합 보안 솔루션을 제공하는데 있어 전문성을 보유하고 있습니다.
- 포트폴리오는 Cisco® ISE(Identity Services Engine) 계획 및 설계 서비스, CISCO의 보안 마이그레이션 서비스로 구성됩니다.

Learn more here

최적화 서비스

- 4가지 계층 : 네트워크, 보안, 데이터센터 및 클라우드, 서비스 제공업체 모빌리티 최적화의 네 가지 계층입니다.
- 규정을 준수하면서 네트워크 및 데이터 보안을 유지하기 위한 Work

Learn more here

자문 서비스

- 사람, 프로세스, 데이터, 사물 간의 연결을 보호하려면 보안이 IOT 처럼 널리 퍼져 있어야 합니다.
- 포트폴리오는 리스크 및 규정준수, IoE 보안, 사고대응 자문 서비스로 구성됩니다.

Learn more here

관리형 서비스

- 모니터링 및 관리부터 포괄적인 위협 솔루션에 이르는 보안서비스와 함께 고객의 요구에 맞게 맞춤 설정할 수 있는 호스팅 서비스를 제공합니다.
- 포트폴리오는 세가지 계층의 위협 분석으로 구성됩니다. Essential, Enhanced, Premier

Learn more here

인시던트 대응

- 공격자를 식별하고, 상황을 포함한 범위, 근본 원인을 파악하고, 근본적인 문제 해결을 위한 전략을 설계하기 위한 계획을 수립합니다.

Learn more here

Cisco Implementation Services

Implementation Services

Plan

- 대화형 인터뷰
- 네트워크 구성도 분석
- 요구 사항 정의, 도입 계획 수립

Design

- 아키텍쳐 설계 검토, 검증
- 설계 및 구성 문서화

lement

- 구현 또는 마이그레이션 활동
- 솔루션 구현 검증

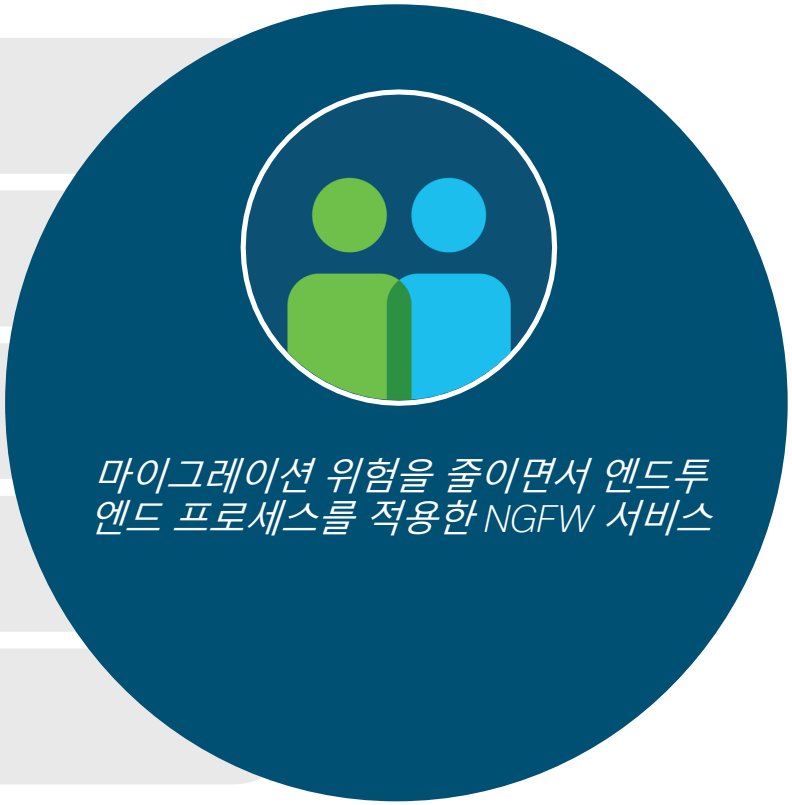
Benefits

- 검증된 사례를 통한 신속한 구현
- 전문가의 계획으로 다운타임 최소화
- CISCO이 방대한 경험을 바탕으로 구축 중 구축 후 위험과 문제 최소화
- 새로운 보안 기술의 성능 최대화
- 프로세스 개선을 통한 ROI 증대

Cisco Implementation Services(1/2)

NGFW(IPS) Migration Services

- 마이그레이션 계획 및 설계
- 마이그레이션 확인 및 지원
- 지식 이전 및 모범 사례
- 절자 문서 작성 방법
- 마이그레이션 실행



Cisco Implementation Services(2/2)

Firewall Quick Start Program

"Firewall 보안정책 및 운용프로세스 최적화를 통한 보안 수준 강화 및 성능 최적화 운영 환경 확보"

기대 효과

- **보안성 강화** — *불필요 보안정책 개선*
- **방화벽 성능 개선**
- **업무효율성 개선** — *운영프로세스 개선*

Firewall Quick Start Program

- **전문인력**
  - 시스코 전문인력을 보안정책/운영프로세스 최적화
- **Cisco Best Practice**
  - 고객환경을 고려하여 시스코 Best Practice 적용

Firewall 정책 관리 어려움

- **Firewall 룰 정책 정기적 점검 및 최적화**
  - 정책 네이밍 규칙
  - 과다 허용 룰 최적화
  - 임시 적용 룰, 중복 룰, 미사용 룰 최적화
- **다양한 방화벽 사용 환경**
  - 멀티 벤더 Firewall 운영의 복잡성에 따른 가시성 한계
  - 설정 오류로 인한 성능 저하
  - 방화벽 교체에 따른 정책 이관
- **운영 프로세스 준수**
  - DX등 인프라 다양한 보안 환경의 변화
  - 보안정책 신청, 통제 적용 절차의 효율성 검토

고객 환경

- Legacy Firewall
- NG-Firewall
- Multi Vendor
- Virtual/Cloud Firewall

다양한 운영환경에 따른 Firewall 보안정책 최적화 및 운영프로세스 고도화 필요

Case Studies

Security Operations Centre (SOC) Services

Challenge

- 전통적으로 보안에 대한 투자가 부족했던 고객은 이를 개선 하고자 했습니다.
- 고객은 내부 리소스, 공급업체 솔루션, 해외 제공 매니지드 서비스 제공업체가 포함된 복잡한 하이브리드 환경을 가지고 있었습니다.
- 전략 설계에 여러 벤더와 이해관계자가 참여함

Solution

- 향후 3년간 개발을 안내하는 데 사용할 수 있는 적절한 서비스 전략 및 설계 계획 수립
- 조직의 엔터프라이즈 아키텍처 관행에 대한 입력으로 핵심 SOC 기술을 포괄하는 다중 레벨 보안 아키텍처

Outcomes

- **장기전략** – 핵심 SOC 서비스의 개발 및 운영을 가이드하는 서비스 중심 전략
- **세부 서비스 설계** – 여러 벤터와 공급업체를 포함하는 설계에 핵심 서비스를 완전히 명시
- **장기 참조 아키텍처** – 향후 5년 동안 통합 시스템을 가이드하는 기술적 설계

Case Studies

Security Assessments

Challenge

- DDoS 공격에 대한 대응 체계 강화

Solution

- 주요 기반 네트워크 장비에 대한 설정 강화

Outcomes

- **네트워크 보안 강화 레포트** – 주요 기반 인프라에 대한 보안 설정 강화 가이드(DDoS, Management Level 강화)

Challenge

- 네트워크 세그먼트 분리

Solution

- DMZ, 서버팜, 사용자 네트워크 분리

Outcomes

- **아키텍쳐 고도화** – 네트워크 세그먼트 분리를 통한 외부 위협 대응 강화 및 내부 접근 제어 강화
- **보안 시스템 고도화** – 방화벽 기반에서 IPS 등 보안 시스템 구축 및 보안 정책 강화(외부 -> 내부, 내부 -> 내부)

Case Studies

IPS Migration Service

Challenge

- IPS 정책의 주기적인 최적화

Solution

- IPS 정책 현행화
- IPS 정책 최적화를 통한 IPS 성능 및 모니터링 역량 강화

Outcomes

- **IPS 최적화 보고서** – 조직의 시스템에 최적화된 IPS 마이그레이션 보고서

The bridge to possible