# EQST insight

## MDR 서비스를 활용한 기업의 사이버보안 고도화 전략

### ■ 개요

전 세계적으로 사이버 공격이 급증하면서 사이버 보안의 중요성이 커지고 있다. 원격 근무가 늘어나고 디지털 기술에 대한 의존도가 증가하면서 접점이 넓어지고 새로운 취약점이 계속해서 발견되고 있다. 이에 기업이 효과적으로 사이버 보안 대응책을 구현하는 것이 어느때보다 중요한 시기다. 최근, 우리나라의 많은 국민들이 이용하고 있는 금융보안인증 소프트웨어(INISAFE CrossWeb EX V3)의 취약점을 악용한 해킹사고가 발생해 국내 주요 기관 60 여 곳의 PC 210 여 대가 피해를 입었다. 이 소프트웨어는 국내에서 1000 만대 이상이 사용하는 것으로 추정되고 있어 관련 피해가 지속 발생할 것으로 예상되고 있다.

게다가 한국인터넷진흥원(KISA)에 접수된 랜섬웨어 신고 건수는 2018 년 22 건에서 2022 년 325 건으로 14 배 이상 급증했으며, 제조업 분야의 중소기업이 많은 피해를 보고 있는 것으로 알려졌다. 이에 고도화되고 지능화되는 사이버 공격에 대해 기업이 진화된 방어 및 대응 체계로 변화해야 한다는 목소리가 커지고 있다.

MDR 서비스는 기업에 24x7 모니터링, 실시간 위협 탐지/분석 및 보안 사고에 대한 빠른 대응을 제공하는 사이버 보안의 고도화된 분석 서비스다. 이번 헤드라인에서는 MDR 서비스의 개요, 특장점, 구성 요소, 구현 및 실제 사례를 소개한다. 기업이 최근 위협 환경에서 MDR 서비스의 중요성을 이해하는데 도움을 제공하고 사이버 공격의 위험을 줄일 수 있도록 중요한 자산을 보호하기 위한 예방 차원의 인사이트를 제시하고자 한다.

## ■ MDR(Managed Detection and Response) 서비스란?

MDR 서비스는 기술, 프로세스 및 전문 지식을 결합해 24x7 위협 모니터링, 분석, 사고 대응 및 보고를 제공하는 고도화된 사이버 보안 서비스다. 보안 위협을 실시간으로 감지하고 대응함으로써 기업을 사이버 위협으로부터 사전 차단할 수 있도록 지원한다. MDR 서비스는 EDR, NDR, XDR 등 여러 사이버 보안 솔루션을 통하여 위협 탐지 및 공격의 가시성을 제공하고 신속하게 사고 대응이 가능하도록 설계되었다.

위에서 설명한 MDR 서비스의 정의를 간단히 설명하면 다음과 같다.

## ■ MDR 서비스의 특장점

MDR 서비스는 실시간 위협 탐지, 보안 사고에 대한 빠른 대응, 사이버 공격 위험 감소, 사전 예방 등 여러 가지 특장점을 갖고 있어 기업이 사이버 공격으로 인한 피해를 최소화할 수 있도록 지원한다.

① 24x7 모니터링: 네트워크 및 엔드포인트를 지속적으로 모니터링하여 잠재적 위협을 실시간으로 탐지하고 대응할 수 있도록 지원한다. 이를 통해 보안 사고를 탐지하고 대응하는 데 걸리는 시간을 단축하여 공격자의 체류 시간(Dwell Time)을 줄이고 공격의 잠재적인 영향을 최소화한다.

② 고도화된 위협 탐지: MDR 서비스는 고도화된 보안 기술을 활용하여 Zero-day 공격, Fileless Malware 및 내부자 위협을 비롯한 잠재적 위협을 식별하여 광범위한 사이버 위협으로부터 기업을 보호한다.

③ 신속한 인시던트 대응: MDR 서비스는 신속한 인시던트 대응 기능을 제공하여 기업이 보안 이벤트를 신속하게 억제하고 해결할 수 있도록 지원한다. 이를 통해 침해로 인한 피해를 최소화하고 데이터 손실 위험을 줄일 수 있다.

④ 전문가 지원: MDR 서비스는 악성코드분석, 침해사고분석, 솔루션 전문가의 지원을 받을 수 있다. 여기에는 위협 헌팅, 인시던트 대응 및 보안 정책 강화도 지원 대상에 포함된다. 기업은 MDR 서비스의 전문가 지식을 활용하여 보안을 고도화하고 사이버 공격의 위험을 줄일 수 있다.

⑤ 규정 준수: MDR 서비스를 통해 기업은 ISO 27001, PCI DSS 및 ISMS-P 인증을 비롯한 컴플라이언스 요구사항을 충족할 수 있다. 이러한 컴플라이언스를 준수하는 것은 개인정보와 같은 민감한 데이터를 처리하는 기업에 매우 중요하며, MDR 서비스는 기업이 이러한 요구 사항을 충족하도록 지원한다.

⑥ 합리적 비용: MDR 서비스 이용 기업은 값 비싼 사이버 보안 기술에 투자하고 전담 보안 팀을 고용하는 대신, MDR 서비스 제공자의 전문 지식을 활용하여 중요한 자산을 보호할 수 있다.

⑦ 확장성: MDR 서비스는 확장성이 뛰어나 기업의 요구사항 증가에도 유연하게 대응 가능하다. 즉, 기업은 변화하는 위협에 빠르게 대응하고 비즈니스 요구사항을 충족할 수 있도록 보안 서비스를 변경할 수 있다.

위와 같이 MDR 서비스의 특장점을 활용하여 기업은 사이버 공격의 위험을 줄이고 지능화된 공격에 능동적으로 대응할 수 있다.

## MDR 서비스 특장점

**SK쉴더스 MDR 보안 전문가 서비스를 활용하여 보안 수준 향상**

EDR
NDR
XDR
등 솔루션

+

전문가
분석 대응
서비스

+

위협헌팅
침해흔적조사
등 고도화
서비스

### 24 x 7 모니터링

- 잠재적 위협을 실시간으로 탐지하고 대응
- 공격자의 체류 시간을 줄이고 공격 영향을 최소화

### 고도화된 위협 탐지

- Zero-day 공격, Fileless Malware 및 내부자 위협을 비롯한 잠재적 위협을 식별

### 신속한 인시던트 대응

- 숙련된 분석/운영 전문가의 신속한 대응
- 이벤트를 신속하게 억제, 해결할 수 있도록 지원

### 전문가 지원

- 악성코드 분석, 침해사고분석, 솔루션 전문가
- 위협 헌팅, 인시던트 대응 및 보안 정책 강화지원

### 규정 준수

- ISO 27001, PCI DSS 및 ISMS-P을 비롯한 컴플라이언스 준수 요구사항을 충족 가능

### 합리적 비용/확장성

- MDR 서비스 제공자의 전문 지식을 활용하여 값비싼 솔루션, 고급 인력 투자 비용 절감 가능
- 기업의 요구사항 증가에 따라 쉽게 확장 가능

## ■ MDR 서비스의 구성요소

MDR 서비스는 모니터링, 분석, 사고 대응 및 보고와 같은 주요 요소들로 구성된다. 모니터링에는 24x7 위협 모니터링 및 알림이 포함되며, 분석에는 위협의 심각도를 결정하기 위한 상세 분석이 반드시 포함되어야 한다. 인시던트는 즉각적으로 조사를 진행하며, 공격 패턴을 식별하여 분석 결과를 문서로 보고해야 한다.

MDR 서비스는 포괄적인 사이버 보안 솔루션을 제공하기 위하여 고도화된 여러 구성 요소로 서비스를 제공한다. 구성 요소는 다음과 같다.

① 위협 인텔리전스: 사이버 공격에 대비하기 위해 위협 인텔리전스를 활용하여 잠재적 위협을 탐지하고 신속하게 대응을 해야 한다. 위협 인텔리전스에는 보안 위험을 식별하고 판별하는 데 사용되는 최신 사이버 위협, 취약점 및 공격 전술에 대한 정보가 포함된다.

② 사고 대응: MDR 서비스는 차단, 격리 및 상세 분석을 포함한 사고 대응 기능을 제공한다. 이를 통해 기업은 보안 사고에 신속하게 대응하고 공격으로 인한 피해를 최소화할 수 있다.

③ 위협 헌팅: 네트워크 및 엔드포인트에 존재하는 위협을 사전에 찾아내는 위협 헌팅 기능도 포함되어 있다. 이를 통해 시스템 내부에 침투한 위협을 식별 및 제거하여 피해를 예방하고 보안을 강화할 수 있다.

④ 보안 분석: MDR 서비스는 보안 분석을 활용하여 네트워크 및 엔드포인트 활동의 패턴 및 이상 징후를 식별한다. 이를 통해 잠재적 위협을 탐지하고 사이버 보안 조치의 효과에 대한 통찰력을 제공할 수 있다.

⑤ 보고: MDR 서비스는 공격 동향, 취약점 및 보안 개선 권장 사항을 포함하여 사이버 보안 위협 및 사고에 대한 정기적인 보고를 제공한다. 이를 통해 기업은 잠재적 위협에 대한 정보를 지속적으로 얻고 사전 예방적인 조치를 취해 위험을 완화할 수 있다.

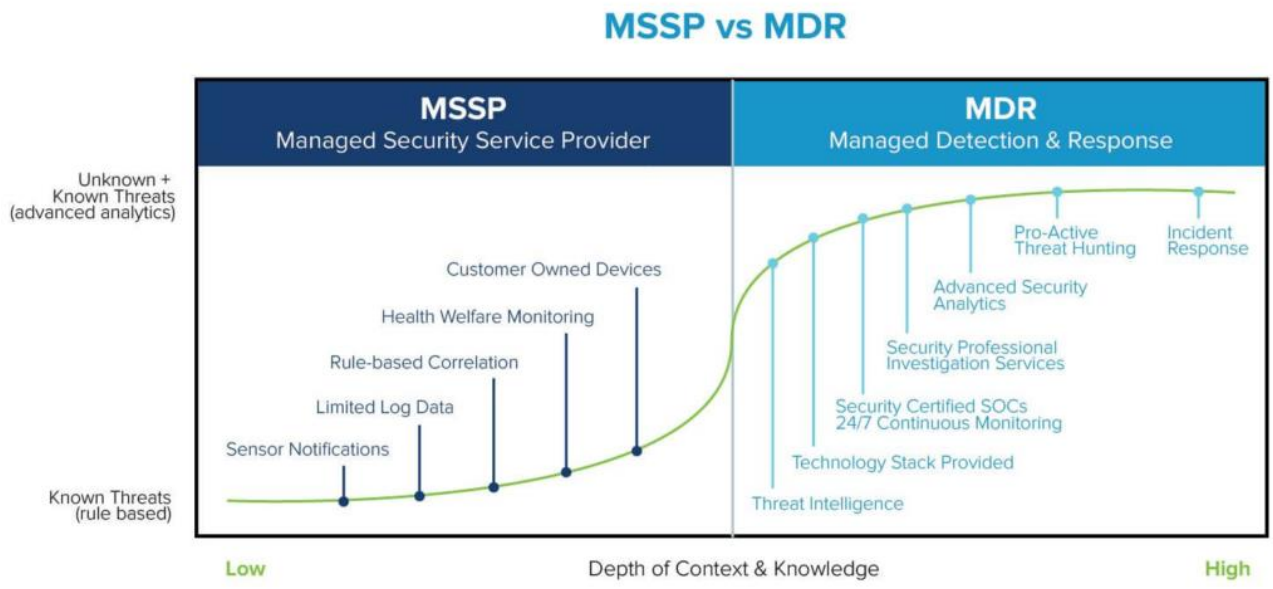
MDR 서비스는 이러한 구성 요소를 활용하여 기업에 사이버 공격 위험을 줄이고 중요 자산을 보호하는 포괄적인 사이버 보안 서비스를 제공한다.

## ■ MDR 서비스 vs 보안 관제 서비스

MDR 서비스는 실시간 위협 탐지의 상세분석 및 구체적인 대응 기능을 제공한다는 점에서 사이버 공격을 방지하기 위해 이벤트 모니터링 및 상관 분석에 중점을 두고 제공되는 MSS (Managed Security Service)와 차별점을 지닌다.

- MSSP(Managed Security Service Provider): MSSP 는 기업에 네트워크 기반 보안 솔루션 관리 및 침입 탐지와 같은 보안 서비스를 제공한다. SIEM(보안 정보 및 이벤트 관리)을 활용하여 네트워크 보안 장비, 서버 및 애플리케이션을 비롯한 여러 경로에서 보안 데이터를 수집하고 분석한다. 또한, 기업이 보안 요구사항을 충족하는 필수 불가결한 서비스이며 MDR 서비스와의 가장 큰 차이점은 지능화된 위협 탐지 및 사고 대응 기능의 제공 여부로 볼 수 있다.

MSS 와 MDR 서비스 사이의 경계가 점점 모호해지고 있지만 결과 측면에서 차이점은 더욱 분명하다. MSS 는 경계를 모니터링하여 알려진 위협을 찾고 자산을 관리하지만 표적 공격은 이를 우회할 수도 있어, MDR 서비스를 통해 보다 고도화된 레벨에서 표적 공격에 대한 대응이 필요하다. 각각의 서비스 특장점을 확인하고 자사 환경에 적합한 서비스를 선택하는 것이 필요해 보이며, SK 쉴더스의 경우 두 서비스를 종합적으로 제공하는 사업자로 각각의 특장점을 최대한 활용해 서비스를 제공하고 있다.




* 출처: https://techgenix.com/mdr-vs-mssp-guide/

## ■ MDR 서비스 구축 방안

MDR 서비스 구축에는 MDR 서비스의 범위 선정, 공급업체 선택, 구축 계획 작성 등 여러 단계가 포함된다. MDR 서비스를 구축하는 데 있어 과제는 비용, 복잡성, 전문 지식의 필요성 등이며, 성공적인 구축을 위해서 모든 이해관계자 참여, 현실적인 구축 계획 수립, 구축 전 MDR 서비스 테스트가 필요하다.

MDR 서비스 구축에는 일반적으로 다음 단계가 필요하다.

① 자체 평가: MDR 서비스를 구현하기 위한 첫 번째 단계는 네트워크 및 엔드포인트에 대한 보안 평가를 수행하는 것이다. 이를 통해 잠재적인 보안 위협, 취약점 및 위협 식별이 가능한지 확인하고 기존 보안 솔루션을 통한 보안 통제가 위험 완화에 효과적인지 여부를 판단하여 자체 평가를 진행한다.

② 계획 수립: 다음 단계는 평가 결과를 바탕으로 MDR 서비스 구현 계획을 수립하는 것이다. 여기에는 특정 보안 요구 사항을 해결하는 데 필요한 MDR 서비스의 구성 요소를 식별하고 구현 범위, WBS 등의 필요한 리소스를 정의하는 작업을 진행한다.

③ 구축: 계획이 완료되면 다음 단계로 MDR 서비스를 구축한다. 이 단계에서는 필요한 하드웨어 및 소프트웨어 구성 요소를 배포하고 시스템을 구성하며, 기존 보안 컨트롤과 통합하는 작업이 포함된다.

④ 모니터링: 구축 후 MDR 서비스는 네트워크 및 엔드포인트를 24x7 로 실시간 모니터링 한다. 이를 통해 잠재적인 보안 사고를 탐지하고 심각한 피해를 초래하기 전 대응한다.

⑤ 위협 및 사고 대응: 보안 이벤트가 탐지되면 MDR 서비스는 차단, 격리 및 상세 분석을 포함한 인시던트 대응을 진행한다. 이를 통해 보안 침해의 영향을 최소화하고 데이터 손실 위험을 줄일 수 있다.

⑥ 보고: MDR 서비스는 보안 동향, 취약점 및 보안 개선 사항, 사이버 보안 위협 및 사고에 대한 정기적인 보고서를 제공한다. 이를 통해 기업은 잠재적 위협에 대한 정보를 지속적으로 받고 사전 예방적인 조치를 취해 위험을 완화할 수 있다.

MDR 서비스 구현은 복잡하고 시간이 많이 소요될 수 있지만 중요한 자산을 보호하고자 하는 기업에게는 매우 중요하다. 이에 SK 쉴더스와 같이 경험이 풍부한 MDR 서비스 프로바이더(Provider)와 파트너 관계를 맺는다면 기업은 효과적으로 보안 체계를 고도화하고 강화할 수 있다.

## MDR Managed Detection Response 구축 절차

[ 사전 준비 프로세스 ] | [ 상시 운영 프로세스 ]

| | 자체 평가 | 계획 수립 | 구축 | 모니터링 | 위협 및 사고 대응 | 보고 |
|---|---|---|---|---|---|---|
| 수행 내용 | **현황 분석 및 평가**<br>▪ 내부 보안 평가를 수행<br>▪ 보안 위협, 취약점 및 위협 식별이 가능한지 확인<br>▪ 기존 보안 솔루션을 통한 보안 통제 여부를 판단하여 자체 평가 | **구축 준비 단계**<br>▪ 보안 요구 사항에 해결을 위한 MDR 서비스의 구성 요소를 식별<br>▪ 구현 범위, WBS 등의 필요한 리소스를 정의 | **구축 및 정책 정의**<br>▪ 필요한 하드웨어 및 소프트웨어 구성 요소를 배포<br>▪ 시스템을 설정 및 기존 보안 컨트롤과 통합 작업 | **보안 확인 단계**<br>▪ 네트워크 및 엔드포인트를 24x7로 실시간 모니터링<br>▪ 잠재적인 보안 사고를 탐지하고 심각한 피해를 초래하기 전에 대응 가능 | **위협 제거**<br>▪ 이벤트가 탐지되면 MDR 서비스는 차단, 격리 및 상세 분석을 진행 인시던트 대응<br>▪ 침해사고의 영향을 최소화하고 데이터 손실 위험 감소 | **운영 대응**<br>▪ 보안 동향, 보안 개선 사항, 보안 위협 및 사고에 대한 정기적인 보고<br>▪ 잠재적 위협에 대한 정보를 지속적으로 얻고 사전 예방적인 조치 가능 |

## ■ MDR 서비스 사례

글로벌 제조 공장을 운영 중인 고객사는 지속적으로 증가하는 멀웨어, 피싱 및 랜섬웨어 공격을 비롯한 여러 사이버 위협에 대한 보안을 강화하고자 MDR 서비스를 구축했다. 동종 업계에서 발생하는 사이버 공격의 위협을 사전에 예방하고 능동적인 보안 체계로 고도화를 할 수 있었다. MDR 서비스는 고객사에 다음과 같은 보안 강화 방안을 제공했다.

① 실시간 위협 탐지: 시간과 공간의 제약없이 해외에서도 실시간 위협 탐지 기능을 통하여 잠재적인 보안 사고를 감지하고 신속하게 대응할 수 있었다.

② 사고 대응: 엔드포인트에서 발생하는 작은 위협에도 상세 분석을 통하여 유입경로 및 영향 범위(내부확산 등)를 파악하고 상시 사고 대응 레벨로 능동적인 대응 방안을 만들 수 있었다.

③ 위협 헌팅: 최근 발생한 침해사고 IoC를 기반으로 위협 헌팅 기능을 제공했으며, 특정 랜섬웨어 공격 집단의 스캔성 접근 등을 원천적으로 차단했다. ASM(Attack Surface Management) 기능을 통해 잠재적인 위협 및 취약점을 사전에 탐지하여 공격을 예방했다.

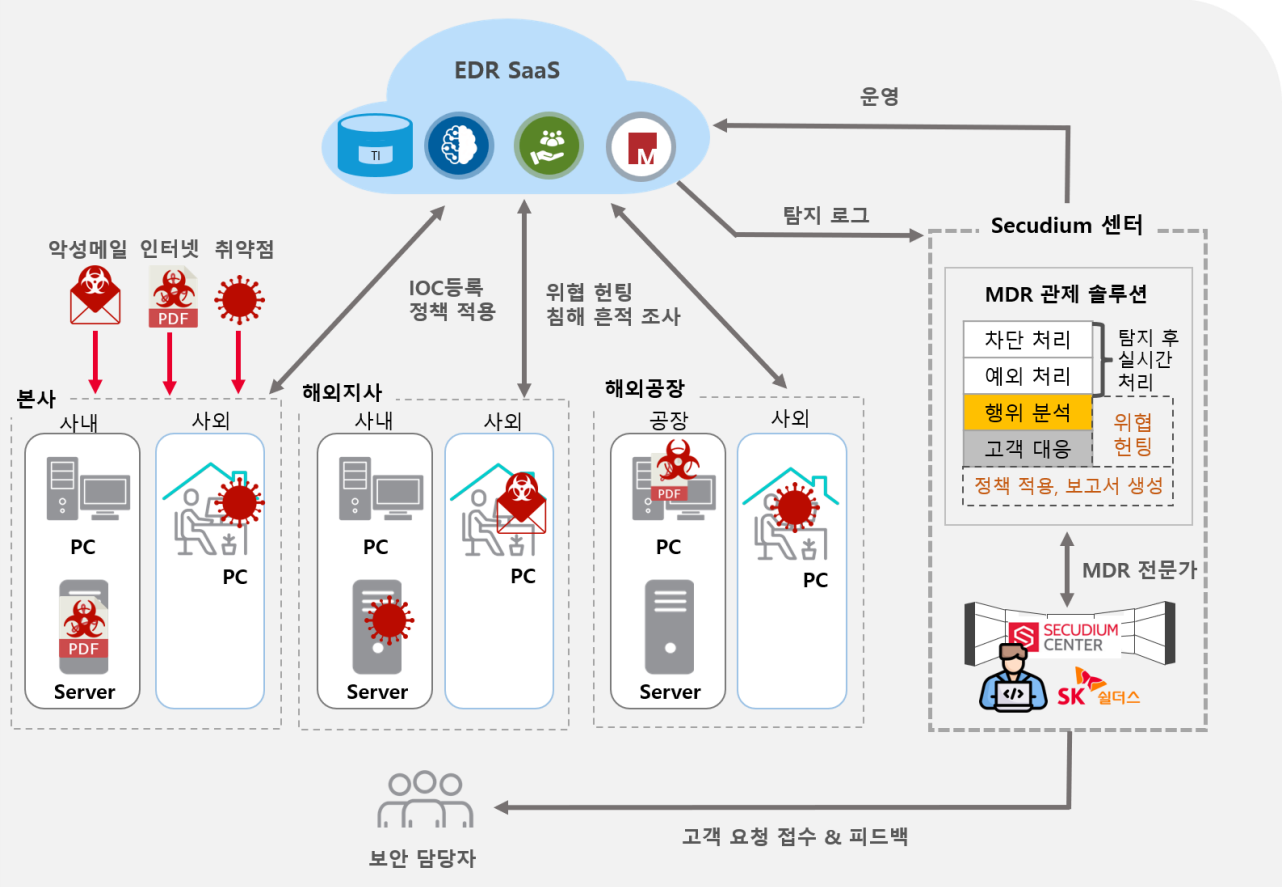
④ 위협 정보 및 보고: 동종 제조업계에서 발생하는 보안 동향, 보안 위협 및 사고에 대한 정기 보고, 서비스 취약점에 대한 정보를 기반으로 지속적인 시스템 점검을 진행하고 있다. 이를 통해 해당 고객사는 잠재적 위협을 완화하기 위한 사전 조치를 취할 수 있었다.

결과적으로 고객사는 사이버 보안 체계를 대폭 강화하고 다양한 공격의 위험을 줄일 수 있었다. 또한 네트워크 및 엔드포인트의 잠재적 위협과 취약점에 대한 가시성을 높여 위협을 최소화하고 비즈니스 운영의 연속성을 보장할 수 있었다.

다음은 위 사례를 기반으로 한 서비스 구성이다.

infosec

## MDR 서비스 구성



## ■ 결론 및 권고 사항

MDR 서비스는 기업이 실시간 위협 탐지 및 대응을 위한 사이버 보안의 필수 구성 요소다. MDR 서비스를 통해 사이버 공격의 위협을 줄이고 전반적인 사이버 보안 수준을 강화할 것을 권장한다. MDR 서비스는 사이버 보안에 대한 포괄적이고 사전 예방적인 접근 방식을 제공하기 때문에 모든 규모와 다양한 기업에 적합한 사이버 보안 서비스다. MDR 서비스는 AI 및 머신러닝과 같은 고급 기술을 활용하여 잠재적인 보안 위협을 실시간으로 감지, 대응 및 완화할 수 있도록 지원한다.
결론적으로 중요 자산을 보호하고 비즈니스 연속성을 유지하고자 하는 기업은 MDR 서비스 구축을 고려해야 한다. 아래 항목 중 3 가지 이상에 해당이 된다면 SK 쉴더스 MDR 서비스팀에 연락 바란다.

① 기업 내부에서 엔드포인트에 대한 위협 분석과 대응이 불가능하다.

② 악성메일이 지속 유입되며 사내에서 랜섬웨어 등 악성코드에 감염된 적이 있다.

③ 시스템에 대한 취약점 진단을 정기적으로 수행하지 못하거나 수행한적이 없다.

④ 재택 또는 출장으로 PC 를 외부에서 사용하는 경우가 있다.

⑤ 방화벽 또는 백신 정도만 운영 중이며 APT 솔루션은 사용하고 있지 않다.

⑥ 보안 사고가 발생하였으나 침해사고 조사를 진행하지 않았다.