ESTsecurity Case Study

ESTsecurity

㈜신세계조선호텔, 전사 알약 EDR 도입

고객사

㈜신세계조선호텔

제품

알약 EDR

도입 규모 및 형태

전 사업장 구축

주요 도입 효과

- ✓ **알려지지 않은 위협 대응**
- ✓ **위협의 근본적인 원인 제거**
- ✓ **위협 인텔리전스로 즉각적인 보안 정책 적용 가능**
- ✓ **보안 관리자의 업무부담 감소**

THE CHALLENGE

기존 글로벌 업체의 EDR 솔루션을 도입해 사용하고 있었으나, 위협의 근본적인 원인을 알 수 없어 잦은 보안 알림으로 오히려 보안 담당자의 업무 부담이 큰 상태였습니다. 때문에 위협에 대한 정확한 정보 제공과 효율적인 대응이 가능한 솔루션이 요구되는 상황이었습니다.

OUR SOLUTION

알약 EDR은 지속적인 모니터링을 통해 알려지지 않은 위협 의심 행위를 선 차단할 뿐만 아니라, 위협 인텔리전스 솔루션인 '쓰렛인사이드(Threat Inside)'와 유기적으로 연동되어 위협 식별 및 상세 분석 정보를 바탕으로 한 전문 대응 가이드로 즉각적인 보안 정책 적용을 지원합니다.

THE RESULTS

도입에 결정적인 역할을 했던 부분은 알약 EDR이 신종 악성코드를 찾아 선 차단하고, 숙주를 찾아내 위협을 완전히 제거할 수 있었다는 점과, 네트워크 차단, 프로세스 종료 등과 같은 대응 프로세스 자동화가 가능해 보안 관리자의 리소스가 최소화된 대응 체계 구축이 가능했던 점입니다.

사이버 위협 대응 솔루션 전문

이스트시큐리티

홈페이지 www.estsecurity.com

대표번호 02-583-4616

솔루션 상담 및 문의

02-3470-2980 biztec@estsecurity.com

ESTsecurity Case Study

ESTsecurity

경찰청,
Threat Inside 분석시스템 IMAS 도입

고객사

경찰청

제품

Threat Inside 분석시스템 IMAS

도입 규모 및 형태

구축형 시스템

주요 도입 효과

- ✓ **자동화된 분석 프로세스로 효율성 증대**
- ✓ **맞춤형 분석 보고서로 빠른 의사결정 가능**
- ✓ **지능화된 공격 및 유사 공격 대응력 강화**

THE CHALLENGE

대한민국 치안 업무를 관장하는 중앙행정기관으로서 사이버 수사 업무와 관련된 파일(앱)의 악성 여부를 검증하고 상세 분석 결과를 활용하기 위한 시스템이 필요했습니다.

OUR SOLUTION

Threat Inside의 분석시스템 IMAS(Intelligent Malware Analysis System)은 지능화된 공격에 대해 침해 정보와 유사한 샘플과의 관계성 및 공격 패턴을 감지하며, 새로운 공격에 대응할 수 있는 정보를 다양한 형태의 보고서 및 통계 데이터로 제공합니다.

일선 수사관이 사건 관련 샘플을 분석 요청할 경우, IMAS는 전문 분석관을 위한 상세 정보뿐만 아니라, 비전문가도 이해하기 쉬운 해석 정보, 수사관이 참고할 수 있는 유사 사건 목록도 함께 제공하여 전문적 데이터를 편리하게 활용할 수 있도록 지원합니다.

THE RESULTS

경찰청 업무 프로세스와 연관된 분석 정보를 제공하여 분석 결과를 효과적으로 활용할 수 있게 되었으며, 동적 분석/정적 분석/유사도 분석 등 다양한 분석 기법을 적용하여 정확도 높은 분석 결과를 얻을 수 있었습니다. 또한 수작업으로 진행되던 업무를 시스템화하여 효율성도 증대되었으며, 실시간 통계 및 맞춤형 보고서를 통해 빠른 의사결정이 가능하게 되었습니다.

사이버 위협 대응 솔루션 전문

이스트시큐리티

홈페이지 www.estsecurity.com

대표번호 02-583-4616

솔루션 상담 및 문의

02-3470-2980 biztec@estsecurity.com

ESTsecurity Case Study

ESTsecurity

국가정보자원관리원(구 정부통합전산센터) 시큐어디스크 1,500유저 도입

고객사

국가정보자원관리원

제품

시큐어디스크

도입 규모 및 형태

1,500 User 구축

주요 도입 효과

- ✓ **문서중앙화를 통한 통합 문서 관리**
- ✓ **자료의 유출 및 유실 방지**
- ✓ **인력 교체로 인한 기록 유실, 업무 공백 방지**
- ✓ **다양한 권한 부여 정책으로 운영 효율 개선**

THE CHALLENGE

국가정보자원관리원은 매년 수많은 정보화 사업으로 인하여 다수의 협력업체 직원이 기관에 상주, 업무를 수행하고, 외주 업체 직원이 반입한 PC에도 프로젝트 산출물을 보관할 수 있다는 점 때문에 문제점이 지속적으로 제기되고 있었습니다. 기존에는 협력업체 임직원이 프로젝트 산출물을 DRM 암호화가 걸린 문서로 업무용 PC에 보관하였다가 프로젝트 종료 시에, 혹은 담당 업무 변경 시, 인수인계 자에게 직접 전달하는 방식이었습니다. 업무 중 자료의 백업 역시 각 업체에 맡겨 문서 유실에 대한 대비책도 필요한 상황이었습니다. 업무 효율과 보안성 개선을 위해 문서 중앙화 체계 도입을 고민하게 되었습니다.

OUR SOLUTION

시큐어디스크는 업무 특성 상 발생하는 인력의 교체 시, 문서 유실이나 업무중단 없이 기존 산출물 전달을 가능하게 합니다. 프로젝트 수행 인력이 개인PC가 아닌 해당 기관 내 중앙 서버의 공유 영역을 할당 받아 문서를 저장하고 업무를 수행할 수 있도록 구축했습니다. 중앙 서버 내 산출물 저장소 역시, 차등적으로 접근 권한을 부여하여 통합 관리 하도록 했습니다.

THE RESULTS

프로젝트 수행 인력들은 개인PC가 아닌 기관 내 중앙 서버의 공유 영역을 할당 받아 문서를 저장하고 업무를 수행함으로써, HDD고장, 악성코드 감염 등으로부터 문서 유실과 유출의 사전 방지가 가능해졌습니다. 중앙 서버 내 산출물 저장소에는 담당 공무원의 접근 권한을 부여함으로써 실시간 문서 공유와 인수인계가 가능해졌습니다. 특히 CD, USB 등 물리적 매체를 통한 문서 전달이 최소화되어 문서 전달 과정에서 보안이 강화되고 "정보시스템 저장매체 불용 처리 지침" 등 각종 보안 컴플라이언스 요건을 충족할 수 있게 되었습니다.

사이버 위협 대응 솔루션 전문

이스트시큐리티

홈페이지 www.estsecurity.com

대표번호 02-583-4616

솔루션 상담 및 문의

02-3470-2980 biztec@estsecurity.com