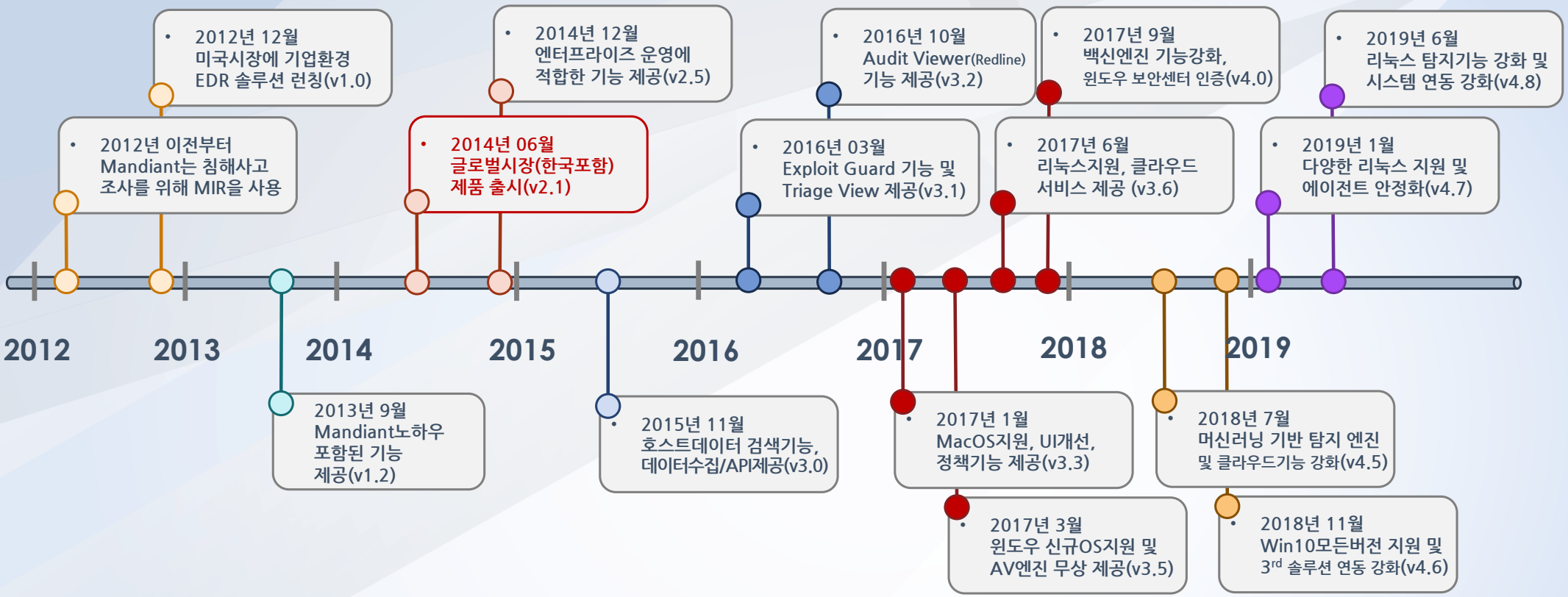
맺음말

차세대 엔드포인트에 대한 FireEye의 자세

오진석 기술총괄 상무

FireEye Korea SE Manager

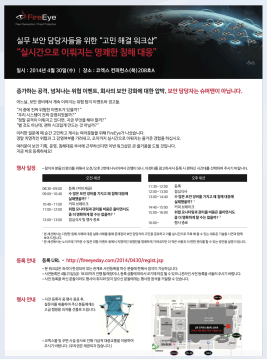
FireEye Endpoint Security



FireEye 한국 지사의 활동

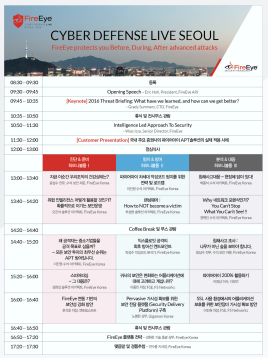
- 2012년 3월 파이어아이 한국지사 설립
- 2014년 3월 엔드포인트EDR 첫 세미나
- 2014년 8월 FireEye Day EDR세션 발표
- 2015년 4월 FireEye Day EDR세션 발표
- 2016년 4월 FireEye Day EDR세션 발표
- 2017년 4월 FireEye Day EDR세션 발표
- 2017년 7월 SGA솔루션스 HX총판 계약
- 2017년 11월 엔드포인트APT 런칭세미나
- 2018년 4월 FireEye Day EDR세션 발표
- 2019년 7월 엔드포인트 시큐리티 세미나
- 2019년 4월 FireEye Day EDR세션 발표

2013



2014

2015

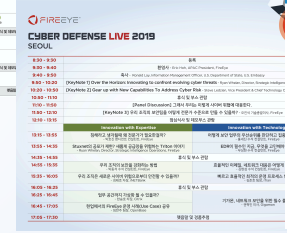


2016

2017

2018

2019



FireEye 한국 지사의 활동

전파지향원

강의 계획 (안)

1. 과정정보	
교육과정명	APT 공격 분석과 방어 솔루션
교육시간	주 3일 (1일 8시간 - 총 24시간)
교육개요	이 과정은 APT 공격 기법과 악성코드 분석 기법을 이해하여 APT 공격을 분석하고 탐지(방어)하는 기법을 학습하는 과정입니다.
교육목적	- APT 공격 및 대응 기법 이해 - 악성코드 분석 기법 이해 - FireEye 솔루션을 이용한 APT 공격 탐지 및 방어 구현
교육대상	- 보안 관리자, 보안 엔지니어 - APT 공격과 악성코드 공격 방법 및 방어 관심있는 사람 - FireEye 파트너 - FireEye 제품을 사용하는 고객사
선수지식	- 시스템과 네트워크 기본 이해 - C 언어 및 프로그래밍 기본 이해 - 어셈블리 기본 이해
실습장비	- FireEye APT 방어 솔루션 - 시스코 UCS 서버 - 시스코 네트워크 장비

2. 세부 교육 내용

단원	강 의 주 제	세 부 내 용	강사
1일차	APT 공격 및 대응 기법	- APT 공격 특성 및 사례 - APT 공격 도구와 기법 - APT 공격 실습 - 솔루션별 APT 공격 대응 기법	
2일차	악성코드 분석 기법	- 악성코드 적용 기법 - DLL 분석 - PE 헤더(PE Header) - 윈도우 안정 프로그램 분석 - 애플리케이션 래핑 후킹 (IAT/EAT/Inline) - 커널 레벨 후킹 (IDT/IRP/SSDT/DKOM) - 악성코드 분석 기법 - 악성코드 디버깅	
3일차	샌드박스를 이용한 악성코드 분석/FireEye 솔루션을 이용한 APT 공격 탐지 및 방어	- 악성코드 분석을 위한 샌드박스 구현 - 샌드박스를 이용한 악성코드 분석 - FireEye APT 방어 솔루션 소개: NX, EX, AX, FX - FireEye 시리즈의 동작원리 이해 - FireEye 시리즈를 이용한 APT 및 악성코드 방어 환경 이해	

전파지향원

세부 교육 내용			
일정	강의 주제		세부 내용
1일차	APT 공격 실습	1	APT 공격 특성 및 사례
		2	솔루션별 APT 공격 대응 기법
		3	APT 공격 실습 환경 구축
		4	Metasploit Framework를 이용한 침투 실습
		5	Meterpreter를 이용한 시스템 제어
		6	RAT 툴을 이용한 침투 실습
		7	SET을 이용한 침투 실습
		8	프로그램 실행 압축(패킹)
2일차	악성코드 적용 기술과 분석 방법	1	악성코드 적용 기술
		2	PE헤더 (프로세스 실행과 메모리 로드)
		3	DLL 인젝션 기법과 구현 방법
		4	API 후킹 실습
		5	악성코드 분석 기법
		6	Sandbox와 Zero Wine을 이용한 악성코드 동적 분석
		7	Ollydbg 사용법
		8	Ollydbg를 이용한 악성코드 정적 분석
3일차	악성코드 침해사고 대응과 포렌식 방법	1	실시간 악성 코드 사고 대응의 필요성 이해
		2	Redline을 이용한 악성코드 관련 증거물 수집
		3	Redline을 이용한 악성코드 관련 증거물 분석
		4	Volatility를 이용한 메모리 포렌식 방법
		5	Volatility를 이용한 악성코드 메모리 포렌식
		6	침해지표(IOC) 생성
		7	침해지표(IOC)를 이용한 증거물 수집과 분석
		8	APT 공격 탐지 요약

플레인비트

세부 강의 내용			
일정	주제	세부내용	강사
1 일차	HX 운영 및 사용법	HX 이해 및 운영에 대해 살펴본다.	파이어아이 수석 컨설턴트
	HX 를 이용한 리버스 커넥션 식별	HX 활용하여 식별하는 방법에 대해 살펴보며,HX 기능 및 구성 방안에 대한 원리를 이해한다.	플레인비트
2 일차	HX 를 이용한 보안 감사	HX 를 이용하여 실제 케이스 분석을 실습한다.	플레인비트
3 일차	평가 1	1 일차에 학습한 리버스 커넥션 식별에 대해 평가한다.	플레인비트
	평가 2	2 일차에 학습한 보안 감사에 대해 평가한다.	플레인비트

플레인비트

구분	교육 전	5/21(화)				5/22(수)				5/23(목)			
		시간	참석대상	주제	주관	시간	참석대상	주제	주관	시간	참석대상	주제	주관
오전	사전 학습	09:30 ~ 10:00	SE	참석환영, 행사의 취지, 내용소개	FE 이동하 이사	09:30 ~ 12:30	SE	HX를 이용한 침해조사 심화 과정(계속)	플레인비트	09:30 ~ 10:30	SE	과정 테스트	FE Korea
		10:00 ~ 12:30	SE	HX를 이용한 침해조사 심화 과정(시작)	플레인비트					10:30 ~ 11:00	SE & Sales	Korea HX 비즈니스 상황 공유	FE 천수홍 사장
										11:00 ~ 11:20	SE & Sales	휴식	
										11:20 ~ 11:50	SE & Sales	HX 비즈니스 지원을 위한 Channel 정책	FE 이동하 이사
										11:50 ~ 12:30	SE & Sales	Endpoint Sales Tool overview	FE 오진석 이사
오후		13:30 ~ 17:30	SE	HX를 이용한 침해조사 심화 과정(계속)	플레인비트	13:30 ~ 17:30	SE	HX를 이용한 침해조사 심화 과정(종료)	플레인비트	13:30 ~ 14:10	SE & Sales	FireEye Endpoint Security 기술지원 시스템	SGA 정진환 부장
										14:10 ~ 15:10	SE & Sales	파트너사별 HX 비즈니스 전략 토의	FE Korea
										15:10 ~ 16:00	SE & Sales	파트너사 전략 발표	FE Korea

플레인비트

파트너 자격증

단순한 제품에 대한 교육이 아닌 침해사고 및 위협 대응을 위한 보안 심화 교육 다수 진행

플레인비트 등 전문가에 의한 교육

“FireEye APT 솔루션이 시장을 선도 했듯이
FireEye Endpoint Security가
차세대 엔드포인트 시장을
이끌어 가겠습니다.”