[K-Shield Jr.] 보안사고 분석대응 세부시간표

구분	과목명	대주제	교육 시간(시간)			
			총	교육내용 별	이론	실습
보안이벤트 대응	운영체제 취약점 이해 및 대응	운영체제 보안 필수요소	40	12	3	9
		취약점에 대한 이해				
		윈도우 시스템의 이해				
		윈도우 보안실무				
		리눅스/유닉스 시스템의 기본이해				
		리눅스/유닉스 보안실무				
		OS서버 취약점을 악용한 취약점 공격사례				
	네트워크 취약점 이해 및 대응	네크워크 기본 이해		16	4	12
		네트워크 보안기술과 최신동향				
		각종 네트워크 보안 솔루션의 이해				
		스니핑 공격 기법의 이해 및 대응				
		스푸핑 공격 기법의 이해 및 대응				
		DDoS 공격 유형과 특징				
		DDoS 공격 실습 및 대응				
	웹 어플리케이션 취약점 이해 및 대응	웹 구성요소의 이해		12	3	9
		웹 기반 공격 기법의 이해				
		웹 보안기술과 최신동향				
		웹 해킹 공격 사례 소개 및 실습				
보안로그분석	로그개요 및 분석 방법론	로그 개요	32	4	1	3
		패턴 매칭				
		보안장비 활용 실습				
		로그 발생 및 공격 이해				
	로그 분석 심화	네트워크 패킷 분석		4	1	3
		패턴 매칭 분석		8	2	6
		난독화 분석기술의 이해				
	시스템 및 보안장비 로그 분석	리눅스와 윈도우 시스템 로그 분석		8	2	6
		보안장비 로그 분석				
	보안장비 이상징후 분석 및 설치 실습	이상징후 분석 개요		8	2	6
		이상징후 분석				
		데이터 시각화 솔루션을 활용한 공격시각화 및 모니터링				
		대용량 데이터 분석 Case 소개 및 실습				
악성코드 분석	리버스 엔지니어링 & 어셈블리 기초	리버스 엔지니어링	32	8	2	6
	악성코드 분석	파일 바이러스 분석(1)				
		파일 바이러스 분석(2)				
		부트 바이러스 분석		8	2	6
	윈도우 프로그래밍	윈도우 프로그래밍의 이해				
	리버스 엔지니어링 실습	Immunity Debugger를 활용한 악성코드 분석		8	2	6
		IDA Pro를 활용한 악성코드 분석		8	2	6
		안티바이러스 분석		8	2	6
디지털포렌식	디지털포렌식과 증거수집	디지털 포렌식 개요	32	8	2	6
		활성 데이터 수집/분석				
		비활성 데이터 수집				
		증거 수집 고려사항				
	디지털 데이터 분석	메모리 수집/분석		21	7	14
		파일 시스템 분석				
		윈도우 운영체제 아티팩트				
		모바일 데이터 분석				
	보고서 작성	분석 보고서 작성		3	1	2
침해사고 분석	침해사고 분석 개요	침해사고에 대한 이해	32	5	2	3
		침해사고 분석 환경 구축				
	침해감염 서버 분석	웹 서버 웹로그 분석		3	1	2
		리눅스 시스템 침해사고 분석				
	침해감염 PC 분석	침해 유입 분석		21	7	14
		윈도우 악성코드 실행 흔적 분석				
		악성코드 은닉/지속 행위 분석				
	침해사고 준비도/대응	침해사고 준비도에 대한 이해		3	1	2
		리눅스 시스템 보안 설정				
		윈도우 시스템 침해사고 준비도 설정				
사이버수사	사이버 수사 관련 법규	디지털 포렌식 관련 법규	8	5	3	2
		최신 사이버 사건 판례				
	사이버 수사관점 이해	증거 수집 및 분석 시 고려사항		3	2	1
		사이버 사건의 법적 절차				
		사이버 사건 상황별 대응				
침해대응팀 (CERT) 구축	침해대응팀 (CERT) 구축	침해대응 조직체계 정의	12	12	4	8
		침해대응 조직 구성				
		침해대응 기본 활동 계획 수립				
		침해사고 접수 처리 계획 수립				
		침해대응 업무 성과 관리체계 수립				
		침해대응 모의 훈련 계획 수립				
		Case 사례분석 및 보고서 작성 / 리뷰				
보안관제 기획/운영	보안관제 기획/운영	보안관제센터 설계	12	12	4	8
		보안관제센터 상세 설계				
		Case 사례분석 및 보고서 작성 / 리뷰				
		보안관제센터 구축				
		보안관제센터 상세 구축				
		Case 사례분석 및 보고서 작성 / 리뷰				
필수교육 이수합계			200	200	60	140