www.igloosec.co.kr

서울시 강남구 삼성동 143-42 원방빌딩 6층 우)135-090 Tel_02) 3452-8814 Fax_02) 3452-8815

SPiDER TM

We provide you with Enterprise Security Management Solution

- CC(CC:Common Criteria, 국제공통평가기준)인증 획득
- 국정원 보안성 검토필 인증 획득
- GS(Good Software)인증 획득
- 정부조달 우수제품 지정 등록

차가운e세상, 안전한e글루

SECURITY

about **SPiDER TM**

완벽한 보안은 기술이 아니라 관리입니다.

SPiDER TM(Threat Manager)은 사용자의 편의성을 추구하면서도 보안인프라의 취약 요소에 대한 지속적인 분석을 통해 위협관리(Threat Management) 개념에 한층 접근한 새로운 차원의 통합보안관리(ESM : Enterprise Security Management) 솔루션입니다.
일관된 정책 아래 이기종 보안장비를 통합하여 관리해주며, 고객의 비즈니스 연속성을 위한 위험관리 전반의 프로세스에 대해 통합적인 지원과 통제를 수행하는 자동화된 시스템입니다.

- CC인증 획득(국가공통평가기준)
  : HP-UX, AIX, Linux, Solaris
- 아시아 최초 CheckPoint OPSEC 인증
- 국가정보원 보안성 검토필 승인
- GS인증 획득
- 위험도추론 침입탐지방법 특허 획득
- 위험도추론 침입탐지시스템 특허 획득
- 로그 샘플링 방법 및 시스템 특허 획득
- 메모리캐쉬를 이용한 통합보안관리시스템 특허 획득
- 3차원 화면을 이용한 통합보안관제시스템 특허 획득
- 통합서버룸관제시스템 특허 획득

효율적인 보안관리를 위한 보다 완벽한 해결책은?

보안관리 시간, 인력, 비용을 줄여주는 ESM이 필요합니다

보안관리의 핵심은 지속적인 통합관리를 통한 예방과 실시간 대응이라는 것이 분명해지고 있습니다. 그러나 해킹기법은 나날이 지능화, 고도화되고 있으며, 제한된 인력과 장비로 인하여 비즈니스의 연속성을 위한 분석과 대응에는 많은 한계를 가지고 있습니다. 그렇기 때문에 기업들은 보안관리를 위한 시간 · 인력 · 비용을 줄여주는 ESM을 필요로 하고 있습니다.
다양하고 복잡한 여러 환경에 적용한 안정성과 구축 경험성을 바탕으로 시장에서 이미 입증되어 온 이글루시큐리티의 통합보안관리(ESM) 제품인 SPiDER TM을 만나 보십시오.

기업의 보안정책을 반영하여 다종 다수 보안시스템을 통합 관제 / 운영 / 관리 함으로써 기업보안 목적을 효율적으로 실현시킬 수 있는 통합보안관제시스템

ESM의 정의, 제1회 정보전 Conference

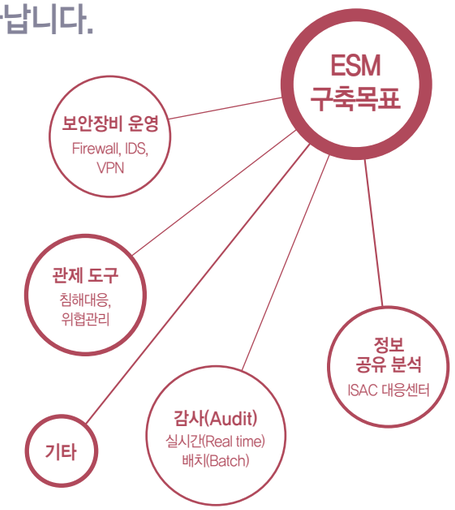
ESM(Enterprise Security Management)이란?

ESM은 기업이 보유하고 있는 각종 보안제품(방화벽, IDS/IPS, VPN, 웹방화벽, UTM, Anti-Virus 등) 및 네트워크 장비(라우터, 스위치 등)와 연동하여 효율적으로 운영할 수 있도록 지원하며, 다양한 위협에 대해 사전/사후 대응을 가능하게 하여 기업의 IT 자산에 대한 가용성, 무결성, 기밀성 보장을 위한 위험관리를 수행합니다.

구축목적에 따라 더욱 확실한 도입효과가 나타납니다.

통합보안관리(ESM)는 구축목표가 명확할수록 도입효과가 높아집니다.
관리의 대상과 범위, 사용자 범위와 이용 형태에 따라 그에 맞는 효과적인 구성을 할 수 있습니다.

- **관리대상 :** 보안장비, 네트워크 장비, 일반서버 등
- **사 용 자 :** 보안관리자, 시스템 운영자
- **구성범위 :** 지역/원격지 네트워크



성공적인 ESM 도입을 위해서는 특별한 Know-How가 필요합니다.

ESM을 도입하기 전 다음과 같은 사항들을 점검해야 합니다.

1 명확한 구축목표를 설정해야 합니다.
ESM의 구축목표가 명확하지 않으면 성공적인 보안시스템을 적용할 수 없습니다. 단순히 보안관리팀 내의 보안장비 운영을 위한 경우라면 SMS(시스템관리 소프트웨어)의 기능이 강화된 제품이 적합할 것입니다.
그리고 감사(Audit)도구의 목적이라면 로그분석 기능이 강화된 제품이 효과가 있을 것입니다. 대규모 관제도구의 목적이라면 관제 프로세스를 지원할 수 있는 기능이 강화된 제품이 필요할 것입니다. 이러한 구체적인 구축목표에 따라 특성을 강조한 보안시스템을 갖추지 못한다면 완벽한 ESM을 활용할 수 없습니다.

2 ESM은 반드시 프로세스가 필요한 관리 솔루션입니다.
즉, 새로운 관리 솔루션의 도입은 기존 프로세스의 변경과 관리가 핵심입니다. 프로세스와 솔루션이 따로 동작하는 것은 결국 명확한 목표를 설정하지 못한 채 실패로 가는 지름길일 수 있기 때문입니다.

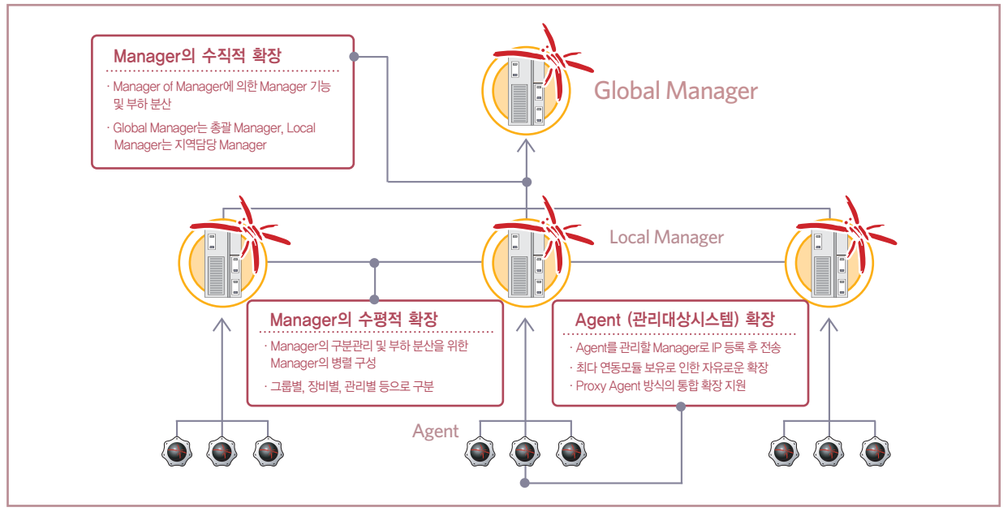
3 단계적이고 체계적인 구축계획이 필요합니다.
현재 나의 조직의 인원, 역량을 고려한 단계적인 목표를 세워 체계적으로 추진하는 전략이 있어야 중장기로 갈수록 견고한 보안체계를 유지할 수 있습니다.

4 전담조직(담당)이 있어야 합니다.
전담조직이란 운영 주체가 명확해야 한다는 의미입니다. 단순히 구매계획에 의거해 운영주체 없이 도입된 제품은 활용도가 미비하여 본래의 구축목적을 상실하기 때문입니다.

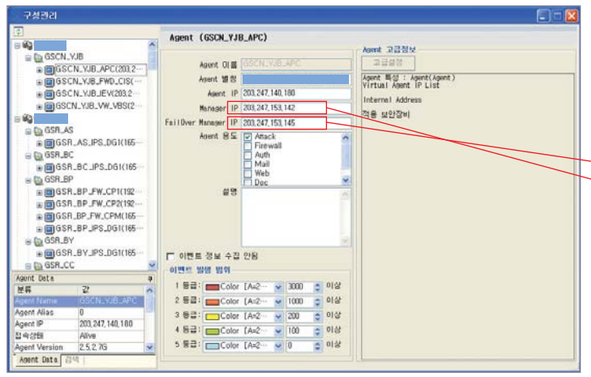
5 ROI는 단기간에 효과를 볼 수 없습니다.
ESM을 구축했다고 곧바로 운영인력이 줄지는 않습니다. 오히려 더 필요할 지도 모릅니다.
ESM의 도입은 보안관리체계의 첫발을 옮긴 것이기 때문에 안정적으로 실행되기까지는 시간이 필요합니다.

명확한 구축목적에 따라 다양한 구성이 가능한 ESM

SPiDER TM은 구축목적에 따라 하나의 지역 네트워크 내에 대규모 인프라를 보유한 IDC 환경이나 위치적으로 여러 곳으로 분산된 대규모 그룹망 환경 등 다양한 모든 구성이 가능하도록 지원합니다.
지역적으로 또는 처리 가능한 용량으로 Local Manager를 분산 구축하여 이벤트의 수집과 분석을 1차적으로 수행토록 하고, 중앙에 Global Manager를 구성하여 전체 총괄 현황 및 최종 분석을 수행토록 합니다.
또한, 대규모 확장을 고려한 Manager의 수직적 확장(Manager of Manager)과 Local Manager의 병렬 확장을 통한 로그 분산 등의 확장방식을 지원하며, Agent 추가에 따른 소규모 확장을 동시에 지원합니다.



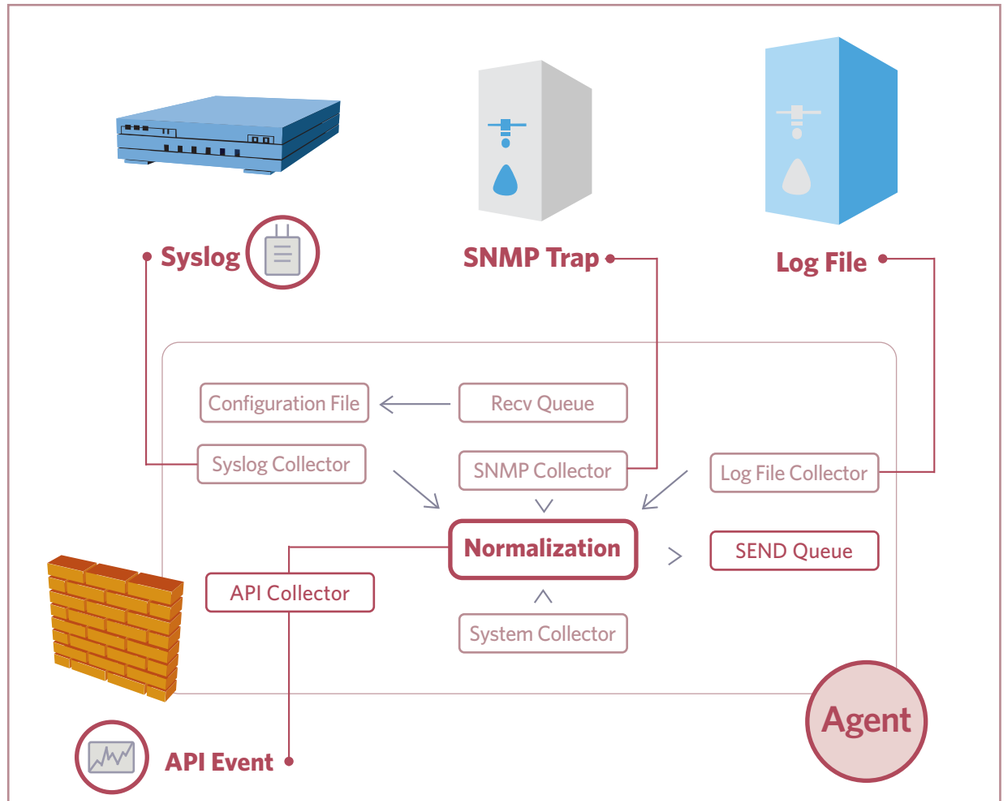
어떠한 장애에도 유동적 대응이 가능합니다



SPiDER TM은 ESM의 무중단 운영과 장애에 안전하게 대응할 수 있는 운영능력을 제공합니다. 별도의 고가 하드웨어나 소프트웨어를 사용하지 않고도 자체 기능만으로 고유업무를 수행할 수 있습니다.

세계 최다 보안장비와의 연동성으로 유동적인 ESM구축

귀사에서 보유하고 계신 보안제품은 어떤 것들이 있습니까?
SPiDER TM은 연동이 검증된 250여 종의 보안 장비 연동 모듈을 보유하고 있습니다. Log File, API, Syslog, SNMP, DB 등 모든 연동 방식을 지원하며, 또한 ISTF의 표준 API를 지원하여 향후 표준화된 인터페이스를 지원하는 보안제품과 별도의 작업 없이 자동으로 연동 가능합니다.



보안장비

방화벽, IDS/IPS, VPN, SSLVPN, Anti DDoS, 웹방화벽, Anti-Virus/Virus Wall, Spam Mail, DRM, PC보안, 서버보안, DB보안, IP관리, 패치관리

일반서버

· Solaris 2.5, 2.6, 7~10
· HP-UX 11i
· AIX 4.3, 5.X, 6.X
· Linux Kernel 2.2, 2.4, 2.6
· Windows 2000/2003/2008, XP/VISTA/7

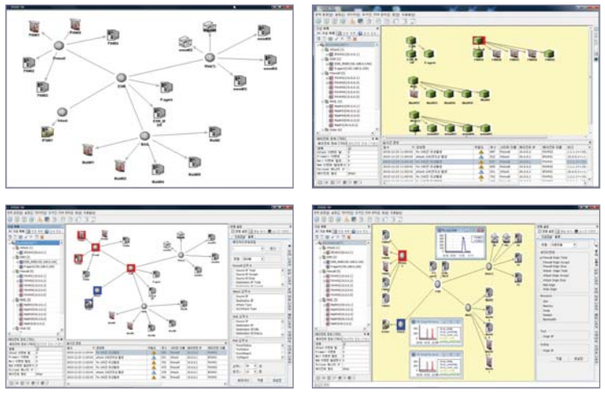
네트워크 장비

· Cisco
· Juniper
· Alteon
· Enterasys
· 3Com

환경에 맞게 손쉽게 설정 가능한 **자유로운 관제화면**

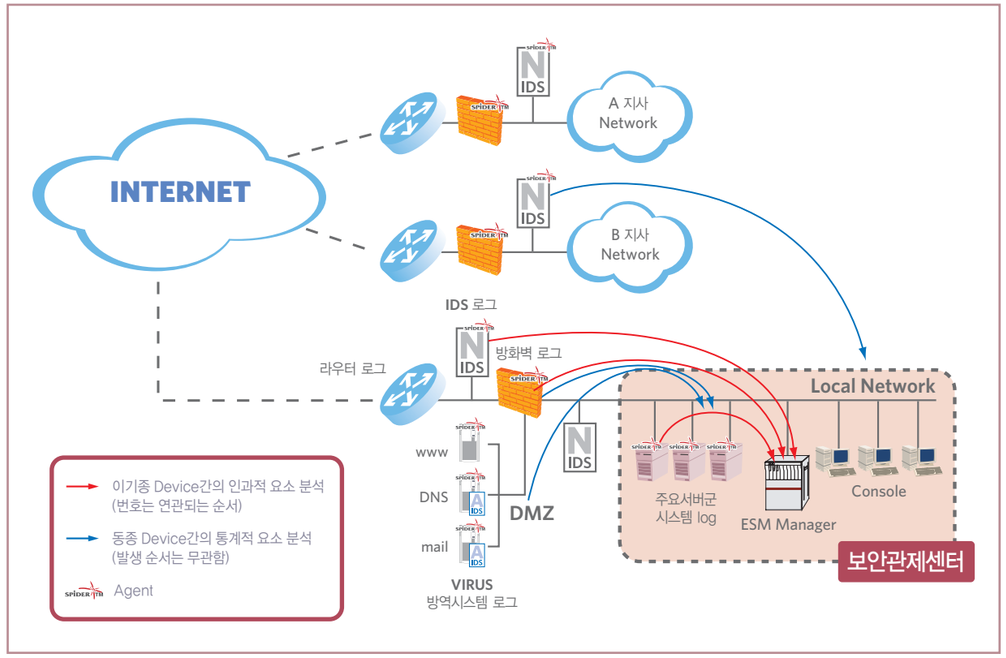
보안시스템은 계층적으로 다양한 사용자들이 존재합니다. SPiDER TM은 지역적으로 업무가 분리된 경우나 보안장비별로 사용자가 분리된 경우 등 모든 사용자가 각 사용자의 환경에 맞게 관제화면을 설정하여 관제화면을 작성, 저장하고 언제든지 불러와서 사용할 수 있습니다.

또한 관제화면은 네트워크 맵과 표, 그래프 등 정보파악에 필요한 항목들도 사용자가 정의하여 만들 수 있으며, 장애 시 또는 경보 발생 시 조건에 따라 표시되는 색상도 자유롭게 선택할 수 있습니다.



정확한 판단을 위한 **자동화되고 객관적인 연관분석**

관제의 핵심은 자동화되고 객관적으로 입증된 분석에 있습니다. SPiDER TM은 이러한 분석이 실시간으로, 또한 특정 기간에 발생한 상황을 정확히 판단할 수 있도록 분석된 결과의 근거 자료를 함께 제공해 드립니다.



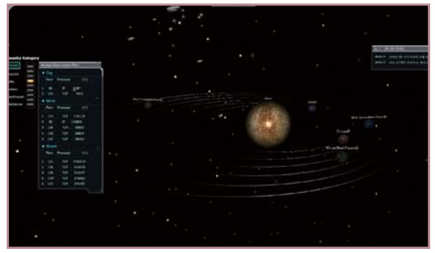
SPiDER TM Option Function

한 차원 수준 높게 3차원적으로 시각화된 보안 이벤트 관제를!

SPiDER TM의 보안 프로세스상에서 발생되는 각종 이벤트에 대한 전반적인 보안 상황을 직관적으로 인지할 수 있도록 구현된 3D 보안관제 console입니다. 특히, 사이버 공격상황에 대해 언제, 어디서, 누가, 어떻게, 무엇을 공격하는지에 대한 상황을 별도의 분석과정 없이 한눈에 파악할 수 있으며, 다양한 보안장비에서 발생하는 이벤트를 실시간 분석하여 해당 기관의 보안 상황 Trend를 파악할 수 있습니다. SPiDER TM 3D console은 실시간으로 네트워크 상황을 인지하던 기존의 시각화 기술을 한 단계 업그레이드함으로써 관제 업무 프로세스를 지원할 수 있도록 영역을 확장한 console입니다.

기관 내의 모든 사이트의 보안 침해 경보 상황에 대한 정보를 직관적으로 분석

- 침해 경보에 대한 유형(웜/바이러스 공격)분류
- 공격자 국가 표시(독일 국기 표시), 공격자 IP, 공격 발생 일시, 공격 대상 사이트를 한번에 표현
- 별도의 분석과정 없이 직관적인 표현이 가능



사이트에서 관리하는 모든 보안장비에서 발생하는 이벤트를 실시간 통계 분석

- 사이트 15에서 관리하는 방화벽 이벤트 중에서 사이트 15로 들어온 허용된 목적지 port에 대해 일간, 주간, 월간별로 실시간 통계 분석 정보를 보여줌

사이트의 특정 보안장비별로 좀더 상세한 분석을 하기 위한 view

- 사이트 15로 들어오는 이벤트 중에서 차단된 목적지 IP에 대해 차단한 방화벽과 공격 국가, 공격 건수를 world map상에 전시
- 어느 국가에서 침입을 시도하는지를 직관적으로 볼 수 있음

SPiDER TM 3D Console 설치 사양

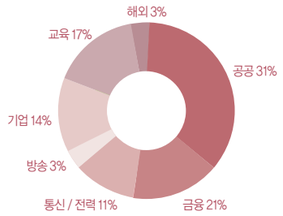
	콘솔(Consol)	미들웨어(Middleware)
운영체제	Windows(2000, XP, VISTA, 7(32bit))	Windows(2000, XP, VISTA, 7(32bit))
CPU	Intel Core2 Quad Q6600 2.4GHz	Intel Core2 Quad Q6600 2.4GHz
Memory	3 GB	3 GB
VGA	GeForce 9000 Series 이상 (video memory : 512 MB 이상)	GeForce 9000 Series 이상 (video memory : 256 MB 이상)
HDD	100 GB	100 GB
NIC	1개(10/100Mbps)	1개(10/100Mbps)

ESM 기능 규격

구분	기능항목		기능내역	비고
시스템 구성 및 성능	시스템 구성	확장성	ESM 통합 및 확장을 위하여 Manager를 계층적으로 분리 구축 및 역할 분리	CM/GM/LM
		안정성	미들웨어 사용을 통한 안정적 구성. 동시에 여러 콘솔이 접속하더라도 성능저하를 최소화하도록 설계	
		가용성	네트워크나 서버 장애 시 무중단 운영을 위한 Agent의 Fail Over 기능 제공	HA없이 자체 기능으로 제공
	Manager	지원 Platform	AIX, HP-UX, Solaris, Linux 등 지원 가능	
	Agent	보안 Agent	방화벽, IDS, IPS, SecureOS, Viruswall 등 보안 이벤트 수집	
		시스템 Agent	AIX, HP-UX, Solaris, Linux, Windows 등 시스템 이벤트 수집	
	DBMS	안정성	상용 DBMS 사용	
	성능	대용량 Agent	2CPU, 8 GB Memory 기준으로 7000건/초 이상 처리능력	
		인공지능 Agent	지정된 CPU 부하 내에서 자동적으로 CPU 부하 조절	
이벤트 수집	이벤트 처리	수집방법	API, SNMP, Syslog, File 등을 통한 실시간 이벤트 수집	동일 이벤트 축약
		필터링	설정된 항목별로 이벤트 필터링하여 설정된 이벤트만 Manager로 전송	
			필터링 항목(보안위험도, IP 대역, 포트, 처리결과 등) 설정 기능	
		기타	수집하고자 하는 특정 파일 사용자 지정 기능	
			파일 내의 특정 패턴 사용자 지정 기능	
관제	관제화면 설정	관제맵 구성	맵편집기를 통한 다단계 맵 구성 기능 제공	
			맵용 아이콘 사용자 지정 기능 제공	
		맵 저장관리	서버 또는 로컬 PC 내에 사용자별 저장/재호출 기능 제공	
		관제화면 구성	관제에 필요한 TOP N 표, 그래프, 실시간 로그창 등을 사용자 지정으로 설정하고 원하는 위치에 구성할 수 있도록 기능 제공	
			그래프의 속성(Line, 3D 등)을 사용자가 지정 변경 가능	
			CPU, 메모리 사용량 등의 성능정보 사용자 지정 기능 제공	
			관제화면을 서버 또는 로컬 PC 내에 저장/재호출 기능 제공	
	이벤트 모니터링	프로파일 관리	특정 공격 유형별 이벤트 모니터링을 위한 조건 설정 후 이를 프로파일로 관리하여 즉시 재사용 가능	
		필터링	이벤트 항목별 필터링 기능 및 불필요 항목 숨김 기능	
			필터링 항목(보안위험도, 공격유형, 출발지, 목적지, 포트 등) 설정 기능	
		예외처리	오류를 줄이기 위한 이벤트 모니터링 예외처리 지정 기능	
	실시간 경보	자동 경보기능	설정된 이벤트에 대해 실시간 알림/경보 기능	
		경보 방법설정	Sound, 팝업창, e-mail, SMS(휴대폰, PDA) 등	
			경보 발생 시 지정된 스크립트 수행 기능 제공	
			동일경보 필터링 및 자동 등급 상향 기능 제공	
			경보 등급, 종류에 따라 맵에 표시되는 색상 사용자 지정 기능	
	장애탐지	과부하 탐지	CPU, Session 임계치 초과 시 탐지	
			초당 발생 이벤트 과부하 탐지	
		Hang-Up 탐지	지정된 시간동안 이벤트 없을 시 탐지	
		기타	평균 사용률 이상/이하의 임계 이격도에 따른 이상 상태 탐지	
			감시 대상 프로세스가 비정상 종료했을 경우 탐지	

구분	기능항목		기능내역	비고
관제	공격탐지	Worm 탐지	Worm 특성을 갖는(Same IP, Port 트래픽 유발) 패턴 탐지	
		불법 접근 탐지	지정된 포트 이외의 불법 사용 포트 탐지	
			중요 시스템 파일 무결성 탐지	
			자체 Agent 기능으로 주요 서버 취약점 스캔 및 원격 접속을 탐지	
		Web 공격 탐지	Web로그를 통한 공격 URL 탐지	Web 서버 연동 시
			Web로그를 통한 SQL Injection 등의 불법 접근 탐지	Web 서버 연동 시
	연관분석	분석조건 설정	이기종 보안장비간 또는 시스템과의 연관성 분석을 하기 위한 조건을 개수에 무관하게 설정 가능	
			사전 룰셋을 등록하여 재사용 가능/필요에 따라 분석률을 적용/미적용/임시미적용 가능	
		분석방법	이기종 보안장비의 모든 이벤트를 메모리상에서 실시간 분석	
			근거 자료는 DB로 별도로 저장/검색 가능	
			오류를 줄이기 위해 조건별로 예외 처리 조건 지정 가능	
분석	로그분석		다양한 조건에 따라 필요한 분석결과를 제공하고, 이 결과를 엑셀 등의 파일로 저장	
	SPiDER TM 3D Console		보안 프로세스상에서 발생되는 각종 이벤트에 대한 전반적인 보안 상황을 직관적으로 인지할 수 있도록 구현된 3D전용 보안관제 콘솔	
			Monitoring view(Main view), 보안 이벤트 범주 view(사이트 view), 보안이벤트 통계 분석 및 경보 분석 view(분석 view), 보안이벤트 통계 분석 및 경보 분석 view(Analysis view) 제공	
침해 대응	침해대응 도움말 관리		침해사고 유형별로 도움말 작성/저장/경보규칙 연계 기능 제공	
			사용자 정의에 따른 대분류, 소분류 구분 가능	
	사고처리	현황관리	경보(침해사고) 유형별 처리/미처리 현황 Viewer 제공	
		침해사고 대응기능	침해사고 처리 이력관리	
			근거 이벤트 검색 기능 제공	
			과거 사고 이력 검색 기능 제공	
			사고 처리/미처리 구분별로 검색 기능 제공	
			사고 처리를 위한 도움말 참조 기능 제공	
자체 보안	암호화		Agent와 Manager, Console간의 통신 암호화 제공(필요에 따라 암호화, 비암호화 선택 가능)	
	상호식별/인증		Agent와 Manager간 SSL 인증서 교환 기능	
운영 관리	권한관리	사용자 그룹 및 사용자별 권한	사용자별 화면별 접근 권한 구분	
			ESM 기능 수행 권한 구분(조회/설정 등)	
	Agent 관리	원격패치	Agent Patch나 업그레이드 시 Manager를 통한 원격 패치기능 제공	
	로그관리	로그보안	보관주기에 따른 로그 보관정책 제공	
		접속로그 관리	ESM 사용자 접속 이력관리	
인증	보안성 평가 인증		국가정보원 보안성 평가 인증을 필한 제품	
기타	언어	다국어 지원	국문/영문/중문/일문 지원	
	스타일	스타일 관리	화면 스타일 사용자 지정 변경 기능 제공	

SPiDER TM Reference



이미 많은 기업이 이글루시큐리티의 SPiDER TM을 만났습니다.

국내 · 외 유수의 기업들이 보다 완벽한 보안문제 해결을 위해 이미 이글루시큐리티의 보안관리 솔루션 SPiDER TM을 선택하였습니다. SPiDER TM은 한 치의 실수도 용납하지 않는 정보보안을 위한 완벽한 파트너가 되어 드릴 것입니다.

국방 · 정부 · 공공

NCIA 정부통합전산센터 · KPIC · 국회사무처 The National Assembly Secretariat · 검찰 · 법무부 · 행정안전부 · 문화체육관광부
보건복지가족부 · 서울특별시 · 세계속의 경기도 · 인천광역시 Incheon Metropolitan City · 대전광역시 · Colorful DAEGU · 광주광역시 · 부산광역시
경상남도 · 경상북도 · 충청남도 · 충청북도 · 전라북도 · 강원도 · 도봉구 · 영주시
상주시 · 연기군 YeonGi-Gun · 인천광역시 동구 · 인천광역시 중구 · 부평구청 · 강화군 · 인천광역시 남구 · 옹진군
KISA 한국정보보호진흥원 · KADO 한국정보문화진흥원 · 건강보험심사평가원 · KLID 한국지적정보개발원 · 한국고용정보원 · 국민건강보험공단 · NPS 국민연금관리공단 · 4대사회보험
중앙선거관리위원회 · ex 한국도로공사 · TS 교통안전공단 · KRA 한국마사회 · KARI · 한국정보사회진흥원 · 기상청 · 노동부
IIAC Incheon International Airport · DLA 운전면허시험관리단 · 질병관리본부 · 외교통상부 · RDA 농촌진흥청 · 환경부 · 우정사업본부 · HF 한국주택금융공사
한국정보통신산업협회 KAIT · 제천시 · OOOO부대 · 기무사령부 · 해군KNTDS · 공군MCRC · 국가기술보안연구소 · 국방전산원

통신 · 전력 · 에너지

KT · KTF · SK 텔레콤 · LG텔레콤 · KTHSolutions · KOPEC · Kdn 한전KDN주식회사 · KPS 한전KPS주식회사
한국동서발전㈜ · wp 한국서부발전㈜ · KOSPO 한국남부발전㈜ · 한국중부발전㈜ · 한국수력원자력㈜ · 한국수력원자력㈜ 원자력교육원

은행 · 증권 · 생보 · 카드 · 유관기관

금융결제원 · 재정경제부 금융정보분석원 · KRX 한국증권선물거래소 · 예금보험공사 · KHFC 한국주택금융공사 · KDIT 신용보증기금 · KB · KB 투자증권
신한은행 · 신한금융지주회사 SHINHAN FINANCIAL GROUP · 한국은행 THE BANK OF KOREA · kdb 산업은행 · 우리은행 · KEB 외환은행 · 농협 · 새마을금고연합회
Standard Chartered SC 제일은행 · 수협 · 전북은행 · 산림조합중앙회 · 신용협동조합중앙회 · KB 국민카드 · 신한카드 · SAMSUNG 삼성카드
대한생명 · 동부생명 · KYOBO 교보생명 · MIRAE ASSET 미래에셋생명 · 동부화재 · 현대해상화재 · Good Company GREEN 그린화재 · 서울보증보험 Seoul Guaranteed Insurance
우리투자증권 · 생명보험협회 Korea Life Insurance Association · NH Card · 전국은행연합회 · citibank

기업 · 방송 · 언론

LG그룹 · LOTTE · Hanwha · 금호아시아나 · HANKOOK · GS 칼텍스 · SSANGYONG MOTOR · KTNET
DAEWOO INTERNATIONAL · Kangwon Land 강원랜드 · CJ 시스템즈 · SoftBank · 가톨릭대학교 가톨릭중앙의료원 · welcome to the soft world 누리콤스퀘어 · INITECH · KBS
SBS · 연합뉴스 · 롯데정보통신 · T money 한국스마트카드

교육 · 비영리

교육사이버안전센터 · KERIS 한국교육학술정보원 · 서울특별시교육청 · 인천광역시교육청 · 대전광역시교육청 · 부산광역시교육청 · 대구광역시교육청 · 울산광역시교육청
광주광역시교육청 · 경기도교육청 · 강원도교육청 · 경상남도교육청 · 경상북도교육청 · 충청남도교육청 · 충청북도교육청 · 전라북도교육청
대전교육정보원 · 강원교육정보원 · 인하대학교 · 경원대학교 · 대구대학교 DAEGU UNIVERSITY · 부경대학교 · 순천대학교 · 부산대학교
충북대학교 · 충주대학교 CHUNGJU NATIONAL UNIVERSITY · 강릉대학교 · 영남대학교 Yeungnam University · 경북대학교 · 명지전문대학 · 안양대학교 · kama 한국자동차공업협회
전국상인연합회 · 서울시립대학교 UNIVERSITY OF SEOUL

해외

DOHA 2006 · ThinkTank systems · KRYPTEC.net · 스토리ASP