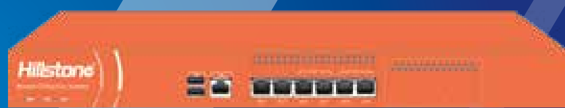
Hillstone I 시리즈
서버 침입 탐지 시스템(sBDS)

I-2850



Hillstone 서버 침입 탐지 시스템(sBDS)은 기존의 시그니처 기반 기술은 물론, 대규모 보안 위협 지능형 데이터 모델링 및 사용자 행위 분석 모델링 등 다양한 위협 탐지 기술을 사용하여 알려지지 않은 보안 위협이나 제로데이 보안 위협 공격을 탐지하고 높은 가치를 지닌 중요한 서버와 내부의 민감한 데이터를 유출이나 도난으로부터 보호하는 이상적인 솔루션을 제공합니다. 능동적인 보안 위협 사냥(threat hunting) 분석 기능과 가시성이 결합된 Hillstone sBDS를 활용하면 보안 관리자가 효과적으로 IOC(침해지표) 이벤트를 탐지하고 보안 위협 공격 킬 체인을 복원할 수 있으며 광범위한 가시성을 통해 보안 위협을 분석하고 완화 방법을 찾아낼 수 있습니다.

지능형 보안 위협 탐지를 위한 포괄적인 위협 상관 관계 분석

오늘날의 사이버 공격은 점점 더 정교한 기법을 사용하여 특정 표적을 대상으로 지속적이고 은밀한 다단계 공격을 수행하므로 경계 탐지를 쉽게 우회할 수 있습니다. Hillstone sBDS는 지능형 악성 코드 탐지(ATD), 비정상 행위 탐지(ABD), 기존 침입 탐지 및 바이러스 검사 엔진을 비롯하여 이미 침입에 성공한 보안 위협 탐지에 중점을 둔 여러 탐지 엔진으로 구성됩니다. Hillstone의 위협 상관 관계 분석 플랫폼은 의심스러운 보안 위협 이벤트 간의 상관 관계와 네트워크 내 다른 관련 정보를 함께 심층적으로 분석합니다. 그 결과 단편적인 정보를 서로 연결하여 의미있는 결론을 도출하고, 높은 신뢰성을 바탕으로 정확하고 효과적인 악성 코드 및 공격 탐지 기능을 제공합니다.

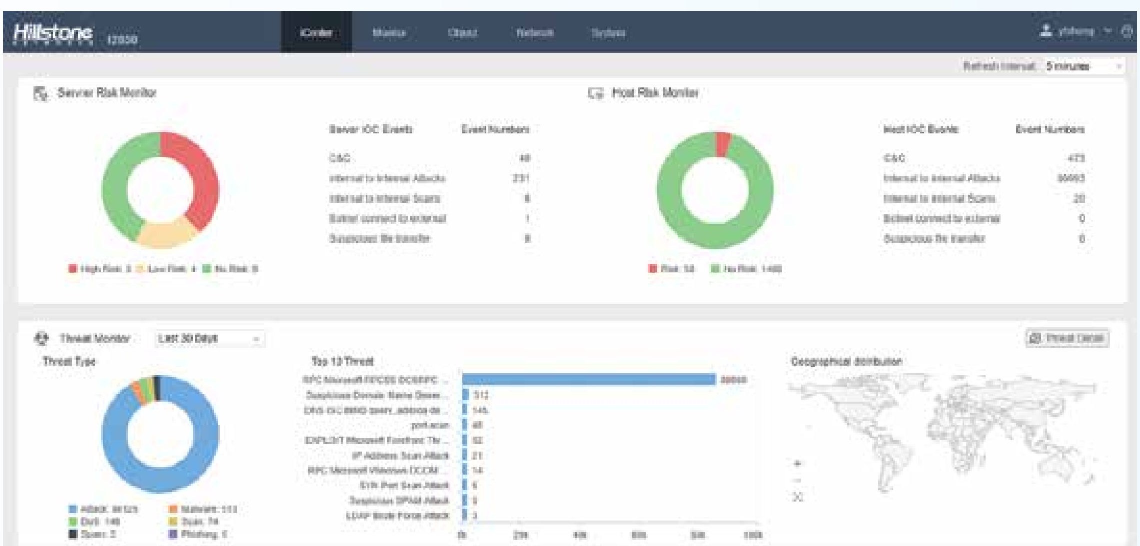


그림 1. Hillstone sBDS I-2850 iCenter 대시보드

www.hillstonenet.kr
Phone: 1-800-889-9860

중요한 서버 및 호스트를 위한 실시간 보안 위협 모니터링

Hillstone sBDS 플랫폼의 주요 기능은 인트라넷 내의 중요한 서버를 보호하고 제로데이에 근접한 공격 및 알려지지 않은 보안 위협을 탐지하며 서버와 호스트 시스템의 네트워크 및 애플리케이션 수준에서 비정상 동작을 찾는 것입니다. 보안 위협이나 비정상 행위가 탐지되면 Hillstone sBDS에서 보안 위협 또는 행위 분석을 수행하고 토폴로지 기반 그래픽 프레젠테이션을 사용하여 보안 위협 세부 정보와 비정상 행위에 대해 광범위한 가시성을 제공합니다. 이를 통해 보안 관리자는 공격의 진행 상황과 양방향 트래픽 추세는 물론, 전체 네트워크 위협 평가에 대해 탁월한 통찰력을 확보할 수 있습니다.

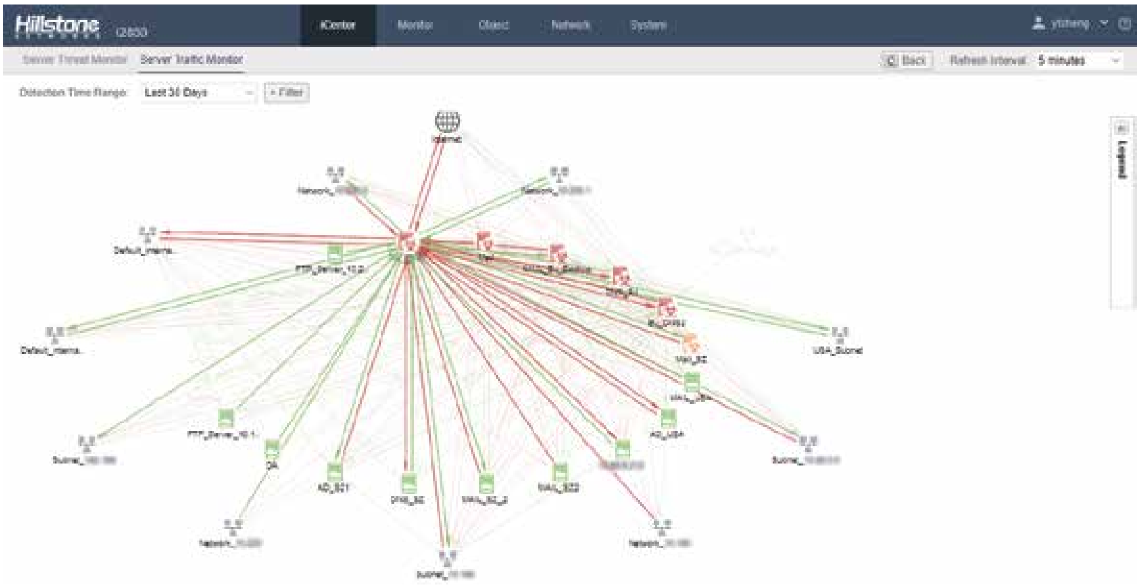


그림 2. 서버 보안 위협 및 트래픽 모니터링

완벽한 IOC(침해지표) 및 사이버 킬 체인

IOC 이벤트는 침입 후 공격 단계에서 탐지되는 보안 위협 이벤트로, 보호 대상 서버 또는 호스트와 직접 연관된 네트워크의 수많은 보안 위협 공격 중에서 별도로 식별됩니다. IOC는 일반적으로 서버 또는 호스트가 손상되었을 가능성이 크며 위협도가 높아 기업 네트워크 내의 중요한 자산에 잠재적으로 더 큰 위협이 될 수 있는 보안 위협 활동을 의미합니다. 핵심 자산의 중요한 데이터를 탈취하려는 공격을 막고 네트워크 내에서 보안 위협이 확산되는 것을 방지하기 위해서는 IOC를 효과적으로 탐지하고 이러한 IOC에 대한 심층적인 보안 위협 탐지를 수행하는 것이 중요합니다. Hillstone sBDS는 IOC 이벤트에 대해 보다 자세하고 광범위한 보안 위협 분석 및 인텔리전스 조사를 수행하여 IOC를 기반으로 공격 체인을 재구성하고 이러한 IOC와 연관된 다른 보안 위협 이벤트를 시간과 공간적인 측면에서 상호 연관시킵니다.

그림 3. 침입 후 보안 위협의 킬 체인 매핑

풍부한 포렌식 정보 및 사전 예방적 완화

Hillstone sBDS 플랫폼은 네트워크 경계에 배치되는 Hillstone E 시리즈 NGFW 및 T 시리즈 iNGFW 장치와 함께 사용하여 보안 위협을 완화합니다. 보안 관리자 또는 네트워크 운영자는 보안 위협 경고를 분석하고 검증하여 IP 주소, 보안 위협 유형과 같은 보안 위협 요소를 블랙리스트 또는 보안 정책에 추가한 후 Hillstone 방화벽과 동기화하여 네트워크 경계에서 앞으로 발생할 동일한 유형 또는 제품군의 악성 코드 공격을 차단할 수 있습니다. 이 방법으로 향후 더 광범위한 네트워크 영역으로 공격이 확산되는 것을 방지할 수 있습니다.

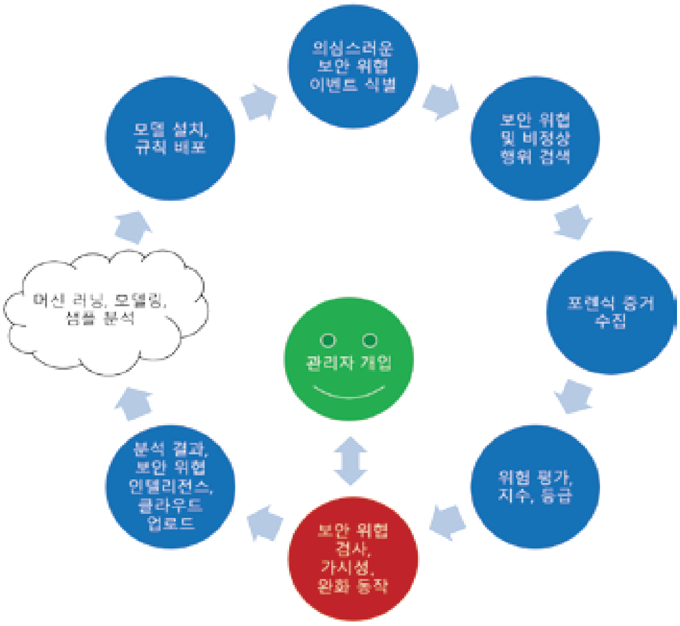


그림 4. Hillstone sBDS 보안 위협 완화 주기

핵심 기능

보안 위협 상관 관계 분석

- 알려지지 않은 보안 위협, 비정상 행위 및 애플리케이션 행위 간의 상관 관계를 분석하여 잠재적 위협 또는 공격 발견
- 클라우드에서 매일 자동 업데이트되는 다중 차원의 상관 관계 규칙

지능형 보안 위협 탐지

- 행위 기반의 지능형 악성 코드 탐지
- 바이러스, 웜, 트로이 목마, 오버플로우 등 2,000개 이상의 알려지거나 알려지지 않은 악성 코드 제품군 탐지
- 악성 코드 행위 모델 데이터베이스 실시간 온라인 업데이트

비정상 행위 탐지

- 기본 L3-L7 트래픽 기반 행위 모델링을 통해 HTTP 스캐닝, Spider, SPAM, SSH/FTP의 취약한 암호와 같은 비정상 네트워크 행위 감지
- DDoS 탐지(Flood, Sockstress, zip of death, reflect, DNS query, SSL 및 애플리케이션 DDoS 등)
- 알려지지 않은 애플리케이션에 대한 암호화된 터널링 트래픽 검사 지원
- 비정상 행위 모델 데이터베이스의 실시간 온라인 업데이트

디셉션 보안 위협 탐지

- 정기적으로 디셉션 모델이 업데이트되는 로컬 디셉션 엔진
- 웹, 문서 또는 데이터베이스 서버 시뮬레이션(FTP, HTTP, MYSQL, SSH 및 TELNET 등의 프로토콜 지원)

침입 탐지

- 8,000개 이상의 시그니처, 프로토콜 비정상 탐지 및 속도 기반 탐지
- 사용자 정의 시그니처, 시그니처 업데이트의 수동/자동 푸시/풀, 통합 보안 위협 백과 사전
- 20개 이상 유형의 프로토콜 비정상 탐지(HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS 등)
- 버퍼 오버플로우, SQL 인젝션 및 크로스 사이트 스크립팅 공격 탐지에 대한 지원

바이러스 검사

- 400만 개의 바이러스 시그니처 데이터베이스
- 온라인 실시간 업데이트
- 압축 파일 검사

공격 탐지

- 비정상 프로토콜 공격 탐지
- DoS/DDoS 탐지(SYN Flood, DNS Query Flood 등)
- ARP 공격 탐지

애플리케이션 식별

- 3,000개 이상의 애플리케이션(IM, p2p, 이메일, 파일 전송 프로그램, 온라인 게임, 미디어 스트리밍 등)
- 구역(Zone), 인터페이스, 위치, 사용자 및 IP 주소 기반의 다차원 애플리케이션 통계
- Android, IOS 모바일 애플리케이션 지원

보안 위협 완화

- 관리자가 보안 위협 이벤트 상태(공개, 오탐, 수정, 무시, 확인) 변경 수행
- 보안 위협 이벤트 화이트리스트(보안 위협 이름, 출발지/목적지 IP, 발생 횟수 등)
- Hillstone 방화벽 플랫폼과 연계하여 보안 위협 차단

모니터링

- 동적 실시간 대시보드 상태 및 상세 모니터링 위젯
- 내부 네트워크 위험 상태 개요(중요 자산 위험 상태, 호스트 위험 상태, 보안 위험 심각도 및 유형, 외부 공격의 지리적 위치 등)
- 중요 자산 및 기타 위험한 호스트에 대한 보안 위협 상태의 시각적 정보(위험 수준, 위험 확실성, 공격의 지리적 위치, 킬 체인 매핑 및 기타 통계 정보 등)
- 네트워크 보안 위협 이벤트의 세부 정보 시각화(이름, 유형, 보안 위협의 심각도 및 확실성, 보안 위협 분석, 지식 기반 및 기록 등)

로그 & 보고서

- 3가지 사전 정의된 보고서 형식: 보안, 플로우 및 시스템 보고서
- 사용자 정의 보고서 지원
- 이메일 및 FTP를 통한 PDF 형식 보고서 전송
- 로그(이벤트, 네트워크, 보안 위협 및 구성 로그 등)
- Syslog 또는 이메일을 통해 로그 전송

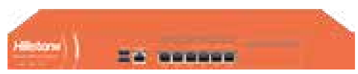
관리

- 내부 네트워크 호스트 및 서버 모니터링, 이름과 운영 체제, 브라우저, 유형 및 네트워크 보안 위협 통계 레코드 식별
- 관리 액세스: HTTP/HTTPS, SSH, telnet, 콘솔
- 장치 상태 경고(CPU 사용량, 메모리 사용량, 디스크 사용량, 신규 세션 및 동시 세션, 인터페이스 대역폭, 섀시 온도 및 CPU 온도 등)
- 애플리케이션 대역폭 및 신규 연결 관련 경고
- 세 가지 유형의 경고 지원: 이메일, 문자 메시지, trap
- 지원 언어: 영어

CloudView

- 클라우드 기반 보안 관리
- 웹 또는 모바일 애플리케이션을 사용한 연중무휴 24시간 액세스
- 장치, 트래픽 및 보안 위협 모니터링

제품 사양

Model	I-2850
	
Breach Detection Throughput(1)	1Gbps
Maximum Concurrent Connections (HTTP)(2)	1.5 Million
New Sessions/s (HTTP)(3)	20,000
Form Factor	1 U
Storage	1T HDD
Management Ports	2 x USB Port, 1 x RJ45 port, 2 x MGT
Fixed I/O Ports	4 x GE
Available Slots for Extension Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+
Power Supply	AC 100-240V 50/60Hz
Maximum Power Consumption	250 W
Dimension (W×D×H, mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)
Weight	15.4 lb (7 kg)
Temperature	32-104 F (0-40°C)
Relative Humidity	5-85% (no dew)

모듈 옵션

Module	IOC-S-4GE-B	IOC-S-4SFP	IOC-S-8GE-B	IOC-S-8SFP	IOC-S-4GE-4SFP	IOC-S-2SFP+	IOC-S-4SFP+
I/O Ports	4 x GE Bypass Ports	4 x SFP Ports	8 x GE Bypass Ports	8xSFP	4XFP Extension Module	2SFP+ Extension Module	4GE PoE Extension Module
Dimension	1U	1U	1U	1U	1U	1U	1U
Weight	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.33 lb (0.15kg)	0.44 lb (0.2kg)

참고: (1) 침입 탐지 처리량은 모든 보안 위협 탐지 기능을 설정한 상태에서 양방향 HTTP 트래픽 감지를 통해 측정되었습니다. (2) 최대 동시 연결 수는 HTTP 트래픽을 사용하여 측정되었습니다. (3) 신규 세션 수는 HTTP 트래픽을 사용하여 측정되었습니다.

EX-08.01-sBDS-V2.0-1017-KR-02