Security Intelligence Platform
for All My Threat Management

BLUEMAX TAMS

Threat Analysis & Management System

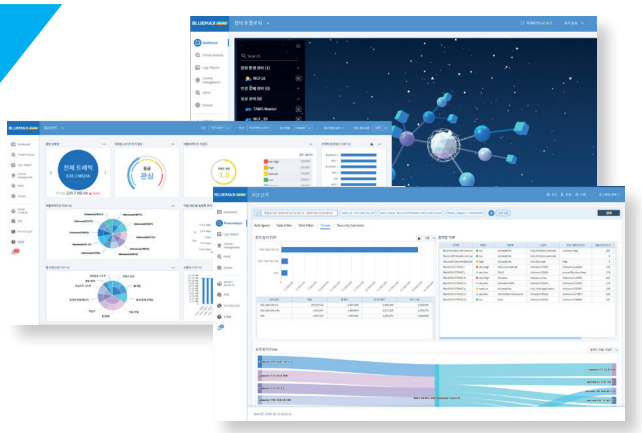
통합 위협 분석, 정책 관리 시스템

SECUI

Threat Analysis & Management System

BLUEMAX TAMS

BLUEMAX TAMS는 분산된 보안 시스템의 통합 위협 분석, 대량 로그 수집, 직관적 통합 설정, 보안 정책 분석 및 최적화로 Security Automation 통합 보안 플랫폼을 제공합니다.



BLUEMAX TAMS 특장점

위협 분석, 통합 설정, 로그 분석, 정책 분석(신청) 모듈을 1 Box 통합

✓ 다양한 기능들을 HW 1 Box에 통합 제공하며, 로그 용량 증가 시 시스템 중단 없는 Cluster 시스템 확장

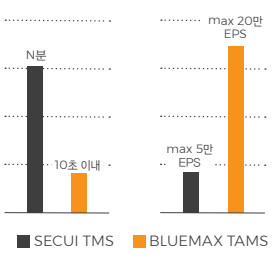
위협 관리 + 통합 설정 + 로그 분석 + **정책 분석** = BLUEMAX TAMS

Big Data 기반 아키텍처로 로그 수집 분석 성능 최대 10배 향상

✓ 기존 제품 대비 로그 저장 성능, 분석/검색 성능 대폭 향상

✓ 1억 건 통계 분석 시 10초 이내 완료, 최대 20만 EPS

✓ 로그 저장 성능 제공 (TAMS 1대 기준)



고가용성 HW 아키텍처로 무중단 서비스 제공

✓ 고성능 SSD 적용

✓ 로그 저장 Raid 구성 기본 제공

✓ 시스템 SW와 보안로그의 저장 공간 분리

Security Automation

실시간 다차원 분석

✓ 시스템 / 위협 현황을 실시간 모니터링 및 다차원 분석하여 다양한 위협 대응 정책에 활용

통합 위협 설정 관리

✓ 실시간 다차원 위협 / 정책 분석 결과에 기반한 직관적인 통합 설정 관리로 편의성 제공

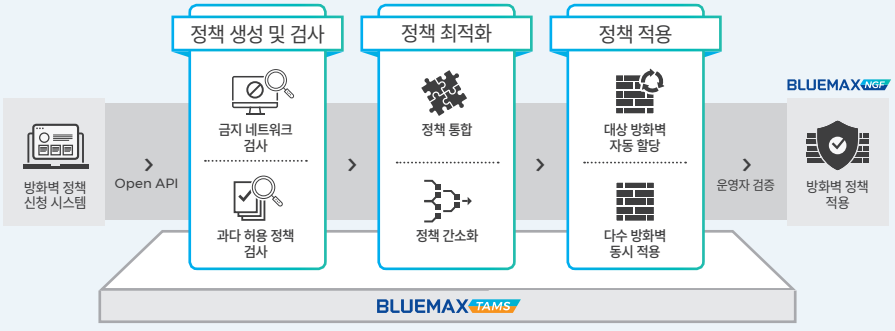
보안 정책 분석, 최적화

✓ 모든 관리 대상 장비들의 보안 정책을 자동 수집 / 유효성 검증 / 최적화하여 휴먼 에러 방지

*보안 정책, 트래픽 경로 분석 기능은 v2.0 개발 예정

보안 정책 관리 자동화

✓ 정책 신청부터 적용까지 보안 정책 관리 프로세스를 자동화하는 One-Stop 솔루션



Software Specification

PAMS
방화벽 정책 신청시스템 연동 지원(IT4U, E-mail 등)
정책 자동 관리 지원
정책 적용 감사 기록 관리(신청 정보별, 적용 정책별)
정책 적용 마법사 기능 지원
정책 Merge 기능 지원으로 정책 최적화 유지
TMS(위협 관리)
수집된 이벤트로부터 위협 분석
종합 상황도 커스터마이징 제공
글로벌(국가별) 공격 통계 리스트
국정원 사이버 위기 경보
해당 공격 Raw Data 보기
예/경보 이벤트 사용자 정의 설정
Central Management
장비 설정 백업/복원
장비 상태(장애) 관리 기능
설정 동기화
장비 자동 등록
통합 스크립트 기능
블랙리스트/ACL 설정

모니터링/대시보드
장비 상태(장애) 실시간 모니터링
전체 장비 트래픽 모니터링
관리 장비 2D/3D 토폴로지 맵 보기
관리 장비의 항목별 TOP 10(그래프 or 정보)
사용자 정의 경고 로그 설정
프로세스 감시 설정
로그/리포트
로그 압축 기능(관리 장비별)
Cluster 구성으로 로그 분산 저장
보안 이벤트 분석/통계를 통한 심층 패킷 분석
즉석, 기간별(주간, 월간, 연간) 리포트 제공
통합 리포트 제공
미사용 정보(객체/정책) 조회
시스템 설정
현재 접속 관리자 정보(현재 상태, 접속 시간)
관리자 설정(IPv4/IPv6, 역할 기반 관리자, 패스워드 정책)
시스템 백업/복구
관리 도구 제공(ping, traceroute, whois)
시스템 무결성 점검

Hardware Specification

BLUEMAX TAMS		100	1000	5000
CPU		4 Core	10 Core	10 Core x 2
Memory		8 GB	64 GB	128 GB
Storage	System	1 TB	256 GB SSD x 2	256 GB SSD x 2
	Log	-	4 TB x 2 / 4 TB x 4	4 TB x 2 / 4 TB x 4 / 4 TB x 6
Interface	10G Fiber	-	(max 2)	(max 2)
	1G Fiber	-	(max 2)	(max 2)
	1G Copper	2	4	4
Power Supply		Single	Dual	Dual
Number of Devices (max)		100	1,000	5,000
Dimension(WxDxH)		1U(426x356x43)	2U(437x648x89)	2U(437x648x89)

SECUI (주)시큐아이

서울특별시 중구 소공로 48 우리금융남산타워
tel 02 3783 6600 **fax** 02 3783 6499 www.secui.com

대표전화 **080-331-6600**
기술지원/침해대응센터 **02-3783-6500**
보안관제센터 **02-3782-4030**
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

CERTIFICATIONS