nurit

정보자산의 이상접속 탐지/차단을 위한

BaroIDS 솔루션 소개서

2021. 5

nurit

Table of Contents

1. 솔루션 개요

nurit

솔루션 개요

BaroIDS 솔루션은 정보자산(서버, 네트워크장비, 보안장비, 저장장치, 데이터베이스, 애플리케이션, 기타)의 **이상접속 탐지 및 차단**에 대한 **현장의 Know-how**을 바탕으로 FDS(Fraud Detection System)를 적용하여 개발된 솔루션으로서 복잡한 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있다.

1. 현장에서 검증된 탐지/차단 Rule

탐지/차단 Rule 을 적용하여 즉시 현장 IDS적용 및 운영이 가능

2. 실시간 로그 수집 가능

다양환 환경에서도 간단한 환경 설정만으로도 쉽게 실시간 로그수집이 가능하여, 복잡한 시스템 환경에 적합

3. 실시간 IP차단 구현

In-Memory 기반 아키텍처로 설계되어, 탐지 즉시 IP차단이 가능함.

4. 축적된 대응체계

현장 경험으로 축전된 대응체계가 시스템화 되어, 대응 및 처리가 용이합니다.

5. Rule Audit & Simulation

발생되는 미탐을 분석하여 신규 Rule을 만들고, 파라미터 조정을 통하여 정탐을 높이는 룰 최적화를 손쉽게 실현

이상접속 탐지/차단

어떤 환경에서던 로그를
실시간 수집분석하여
이상접속 즉시,
IP차단이 가능한
검증된
Intrusion Detection System

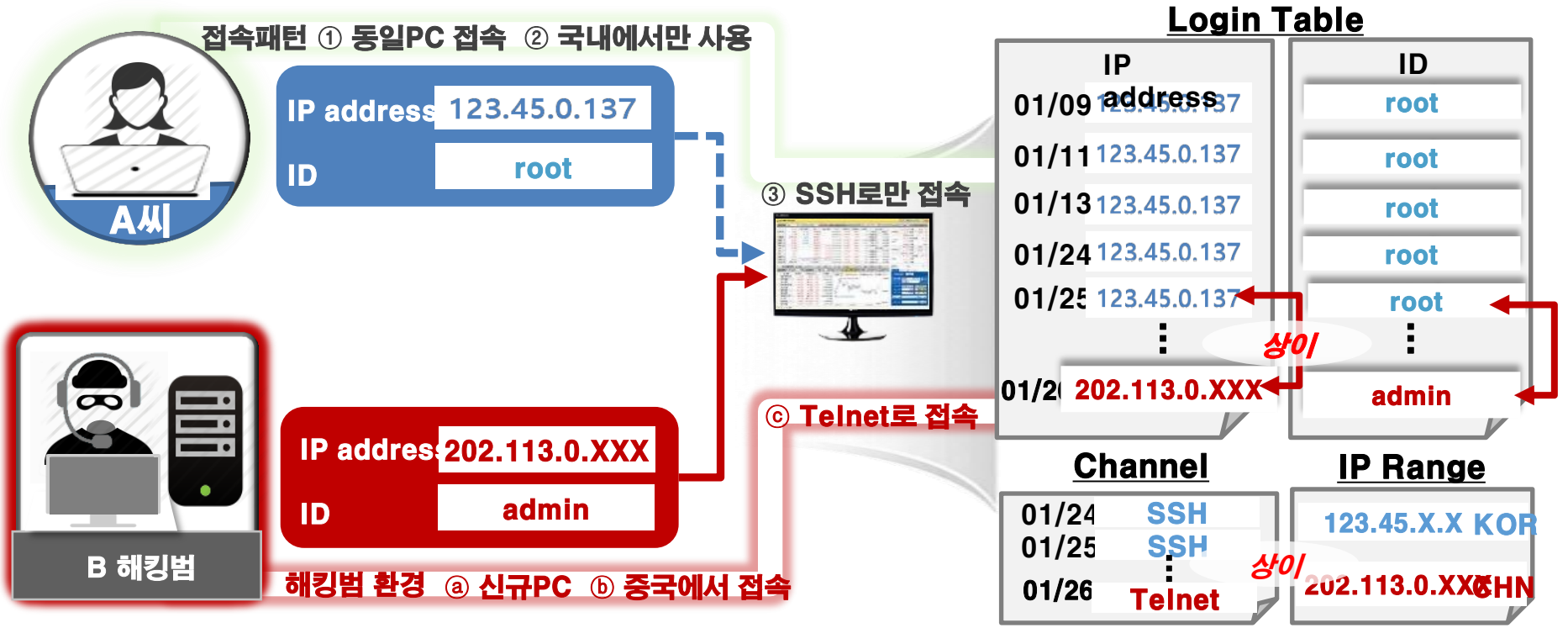
2. 솔루션 특장점

특장점#1 Rule - 조합된 인자기반 탐지/차단 Rule Set

이상접속 Rule은 여러 가지의 침입징후인자가 조합되어 구성됩니다. 실제 사용자의 행동패턴에 대한 축적된 로그를 기반으로 룰을 만들고, 탐지건의 접속 패턴에서 이질성을 감지하여 침입을 탐지합니다.

실제 RULE SET

#1 現접속된 ID의 IP와 호스트명이 로그인 Table에 t-1일(전일) ~T -365(전일) 에 없으면 비정상
#2 現접속된 ID의 IP 주소가 해외 IP면 비정상임
#3 現접속된 ID의 접속매체가 로그인 테이블에 t-1(전일) ~ T-365(전일)에 없으면 비정상임



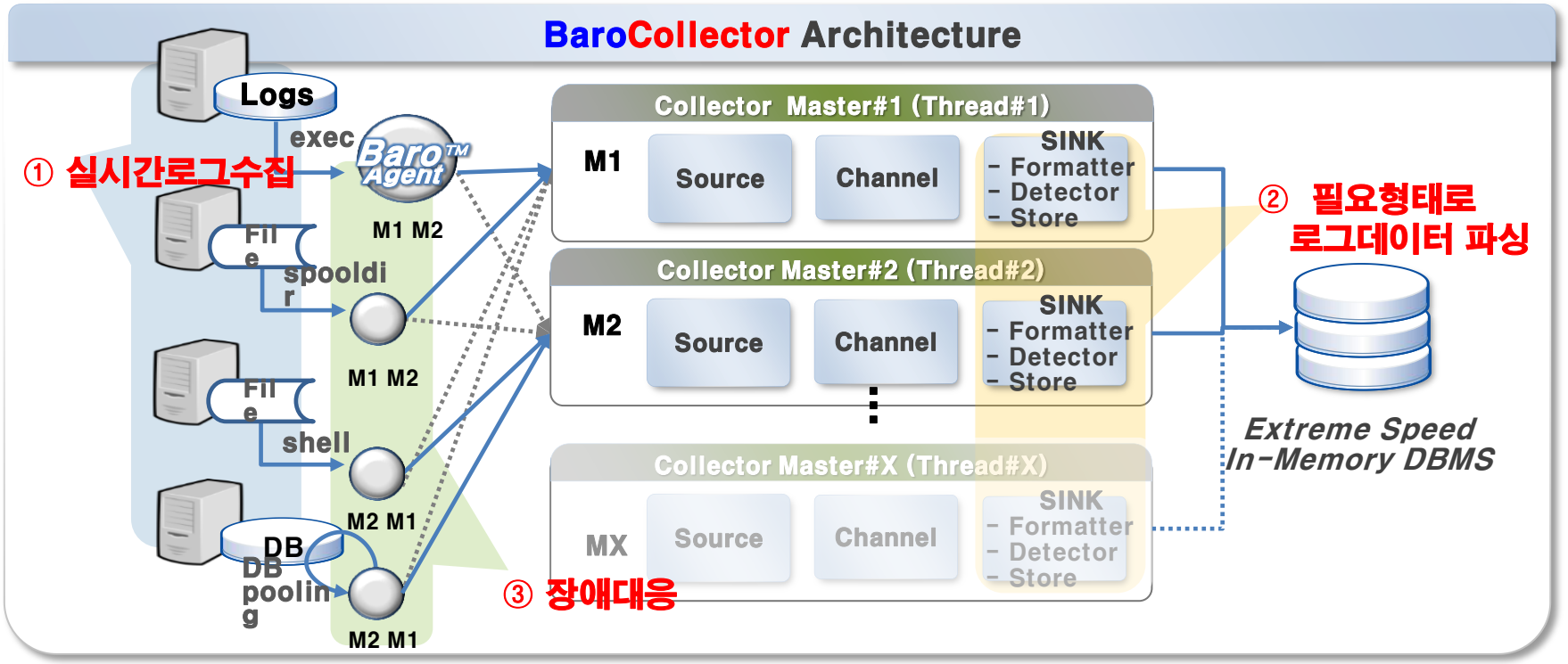
2. 솔루션 특장점

nurit

특장점#2 다양한 Platform을 지원하는 Log-Collector

BaroIDS 솔루션의 또 다른 핵심은 기존 시스템에 변경을 거의 주지 않고 로그를 실시간으로 수집하고, 이를 필요한 형태로 저장이 가능하며, J2EE기반의 Collector로 어떤 환경에서 즉시 로그수집이 가능합니다.

① **실시간 로그수집:** 환경변수 설정만으로 Source 종류에 상관없이 실시간으로 수집 가능
② **필요형태수집 및 저장:** 로그 포맷터를 보유해 환경변수만으로도 비정형/정형에 상관없이 원하는 형태로 저장가능
③ **부하분산:** 순차적 배분(Round Robin), 동적 배분(Random) 가능
④ **장애대응:** 장애 시 이를 감지하여, 다른 Thread (또는 다른 Instance)로 대체 및 비정상 종료시 재기동으로 안정적인 수집 가능

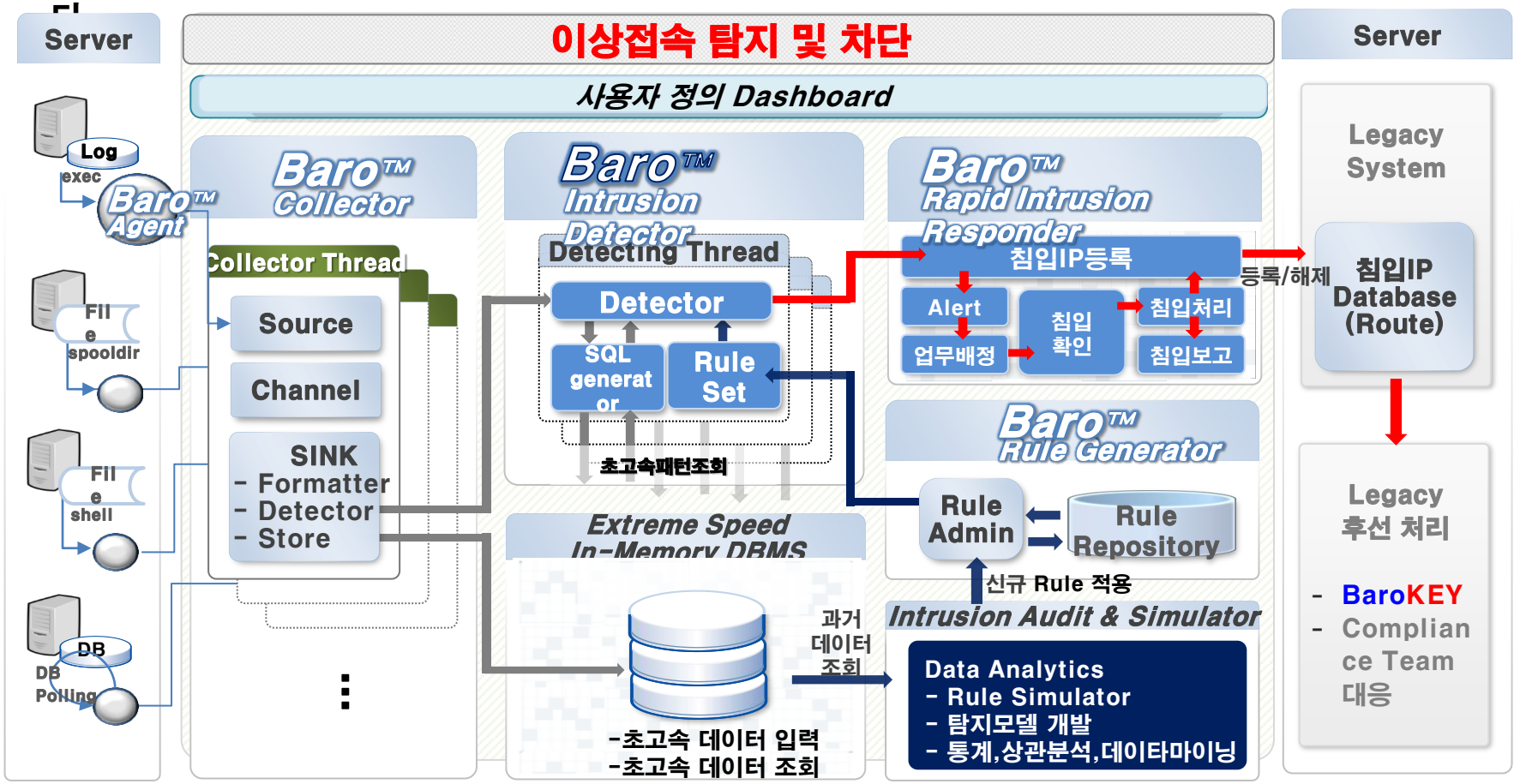


2. 솔루션 특장점

nurit

특장점#3 초고속 인-메모리 아키텍처

BaroIDS 솔루션은 극초고속 인메모리 기반 아키텍처로 설계되어, 이상접속 징후인자를 기반으로 각종 로그발생 후 과거의 로그 프로파일을 빠른 시간에 분석 대조하여 이상접속 징후를 탐지하여 접속을 차단합니다.



2. 솔루션 특장점

nurit

특장점#4 체계화된 침입대응 Process

이상접속은 지금까지의 전혀 다른 형태로, 진화하는 해킹범들의 수법을 지속적으로 모니터링하고 이를 BaroIDS 솔루션에 반영해야 함. 이상접속 탐지 및 차단은 현장에서 검증된 체계를 기반으로 운영되어, 분석→운영→대응이 선순환으로 운영되어 계속 변화하는 서버 해킹에 효과적 대응이 가능 합니다.

이상접속분석

- 신규사고유형접수 (컴플, 자체)
- 침입유형관련 이상접속 인자 분석
- 신규차단/탐지룰 생성
- 기존 사고사례 기반 Rule Simulation

IDS운영

- 신규/차단/탐지 Rule 가동
- 기존/신규차단/탐지 Rule 적정성 모니터링 (오탐↓ / 정탐↑)

이상접속 발생시 대응체계

침입대응 #1
차단룰에 의한 차단

▶

침입대응 #2
접속 Profile 기반 초동분석

▶

사고대응 #3
- 오탐: 사고해지
- 정탐: 접속차단

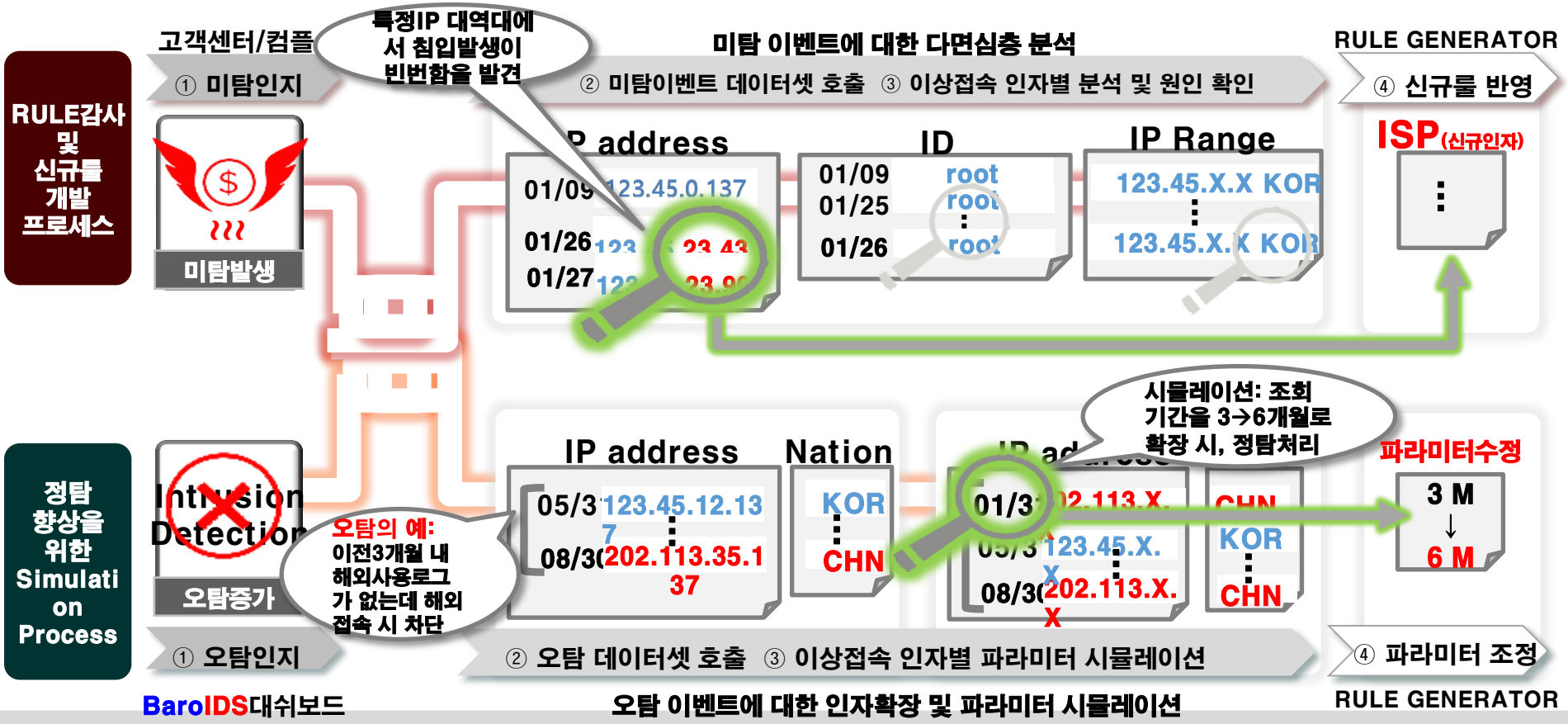
▶ 침입대응 #4 침입보고

▶ 침입보고서 작성

2. 솔루션 특장점

특장점#5 Rule Audit 및 Simulation

이상접속은 지속적으로 진화하기 때문에 Rule도 이에 따라 지속적으로 추가되어야 함. 또한 오탐 증가로 인한 여러 문제가 발생하기 때문에 이를 개선할 수 있는 도구가 필요하며, 이상접속 탐지/차단은 수집된 데이터를 분석하여 추가적인 신규룰 개발이 가능하고 시뮬레이션을 활용하여 정탐률 향상이 가능합니다.



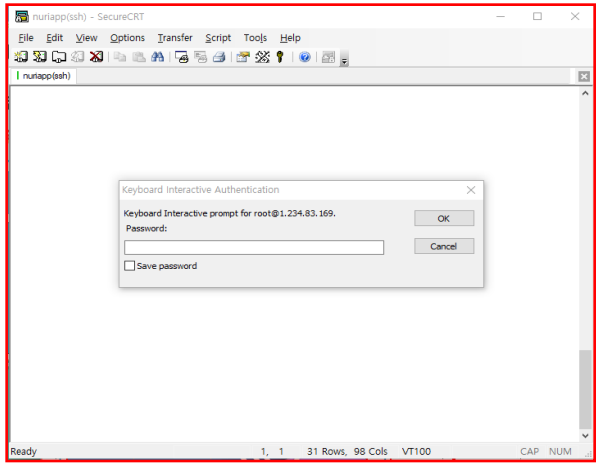
3. 보안 전략

BaroSolution 솔루션의 3단계 보안 전략(Linux/Unix)

BaroSolution 솔루션의 보안 전략은 3단계로 구성이 되며, 1단계는 전형적인 기본 보안(ID/Password), 2단계는 일회용 인증키를 적용한 보안의 전략적인 구성, 3단계는 이상접속 탐지 및 차단을 통한 불법적인 정보 자산의 접속 제어로 구성되어 있습니다.

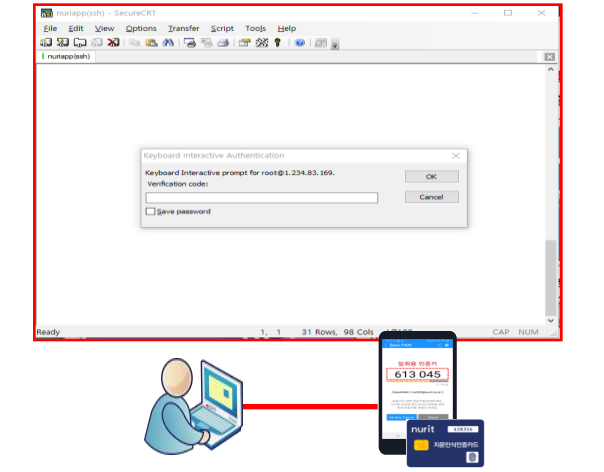
1단계

기존의 전형적인 기본보안
(ID / Password)



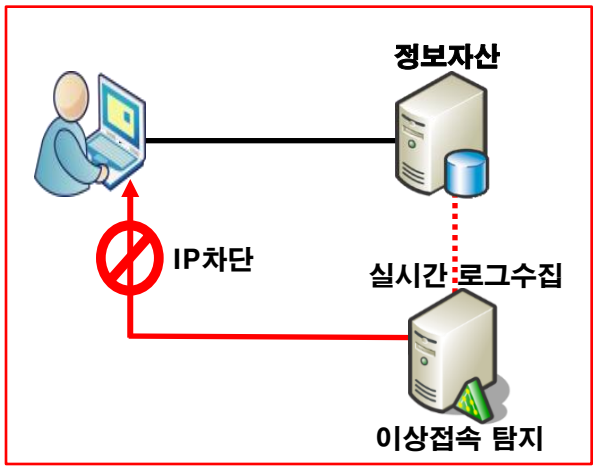
2단계

지문인식 인증카드나
스마트폰 앱을 이용하여
2세대 인증키를 부여 받아 입력
(일회용 인증키)



3단계

각 정보자산의 실시간 로그수집
및 Rule을 적용하여 비정상적인 접속을
탐지 및 IP 차단
(이상접속 탐지 / 차단)



3. 보안 전략

BaroSolution 솔루션의 3단계 보안 전략(애플리케이션)

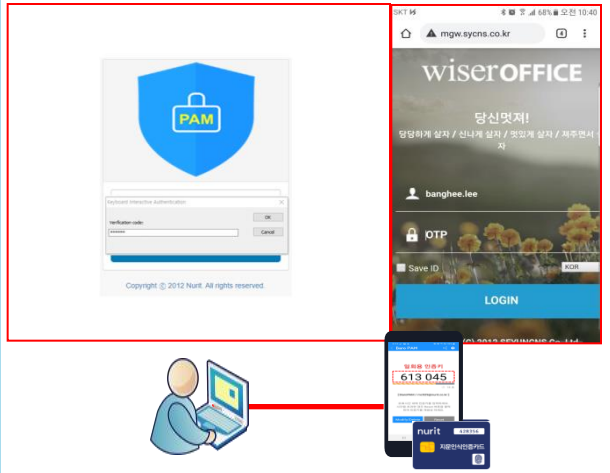
BaroSolution 솔루션의 보안 전략은 3단계로 구성이 되며, 1단계는 전형적인 기본 보안(ID/Password), 2단계는 일회용 인증키를 적용한 보안, 3단계는 이상접속 탐지 및 차단을 통한 불법적인 정보자산의 접속 제어로 구성되어야 합니다.

1단계

기존의 전형적인 기본보안
(ID / Password)

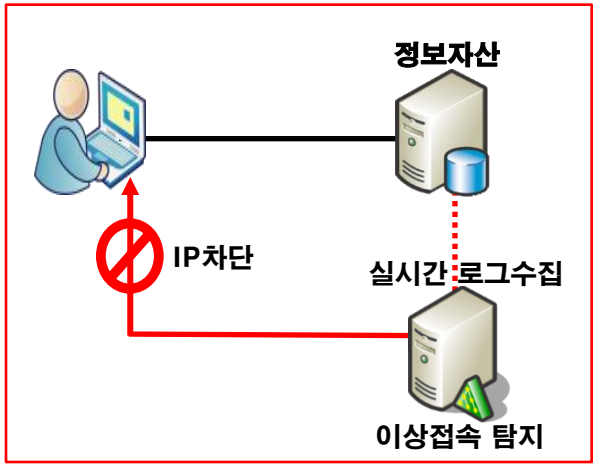
2단계

지문인식 인증카드나
스마트폰 앱을 이용하여
2세대 인증키를 부여 받아 입력
(일회용 인증키)



3단계

각 정보자산의 실시간 로그수집
및 Rule을 적용하여 비정상적인 접속을
탐지 및 IP 차단
(이상접속 탐지 / 차단)

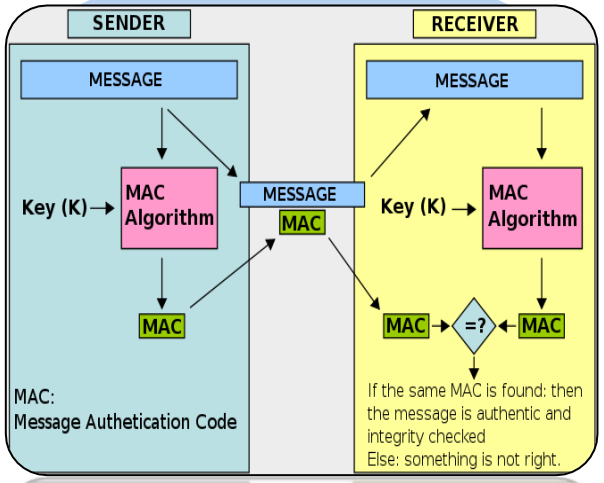


4. 솔루션 구성

솔루션 구성

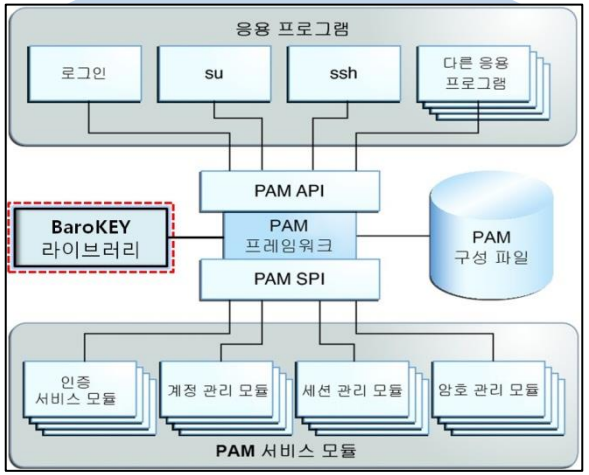
BaroSolution은 다음과 같이 BaroKEY, BaroPAM, BaroIDS를 접목시킨 정보자산에 대한 접근제어 2차 인증(추가 인증) 및 이상접속 탐지/차단 시스템으로 구성되어 있다.

일회용 인증키(2nd 인증키)



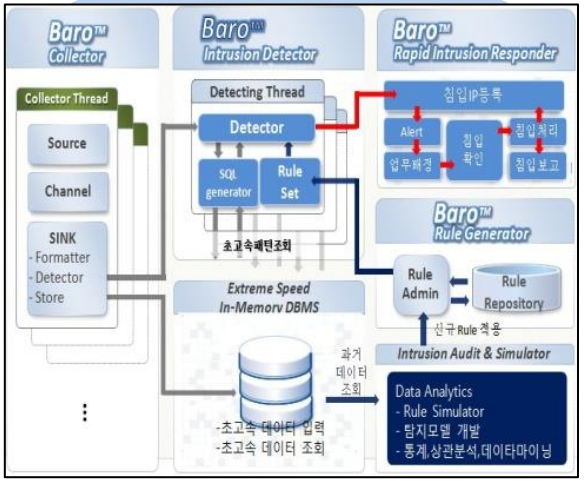
- -512bit 표준해쉬함수(HMAC-SHA512) 사용
- -금융감독원에서 권장하는 Time-sync 방식
- -동적 SEED 암호화 알고리즘 방식
- -인증서버가 별도로 필요하지 않는 소프트웨어 방식(2세대 인증키, 소프트 인증키)
- -인증키 생성주기(3~60초) 개별 부여
- -2-팩터/2-채널 인증의 비밀번호 대체 지원
- -하드웨어 인증키와는 달리 영구적 사용가능
- -다양한 응용프로그램 및 연동 개발의 편의성 제공(Java, C 언어로 된 API 연동)

정보자산 접근제어(PAM)



- -PAM+2차 인증(BaroKEY)+이상접속 탐지/차단(BaroIDS) 방식의 정보자산 접근제어
- -인증서버 및 접근제어 서버가 필요 없는 소프트웨어 방식
- -기존 네트워크 장비의 설정 변경이 필요 없음
- -2차 인증에서 허용 및 제외할 수 있는 계정에 대한 ACL기능
- -정보자산별, 애플리케이션별, 계정별로 일회용 인증키 및 인증키 생성주기(3~60초) 개별 부여

이상접속 탐지/차단(IDS)

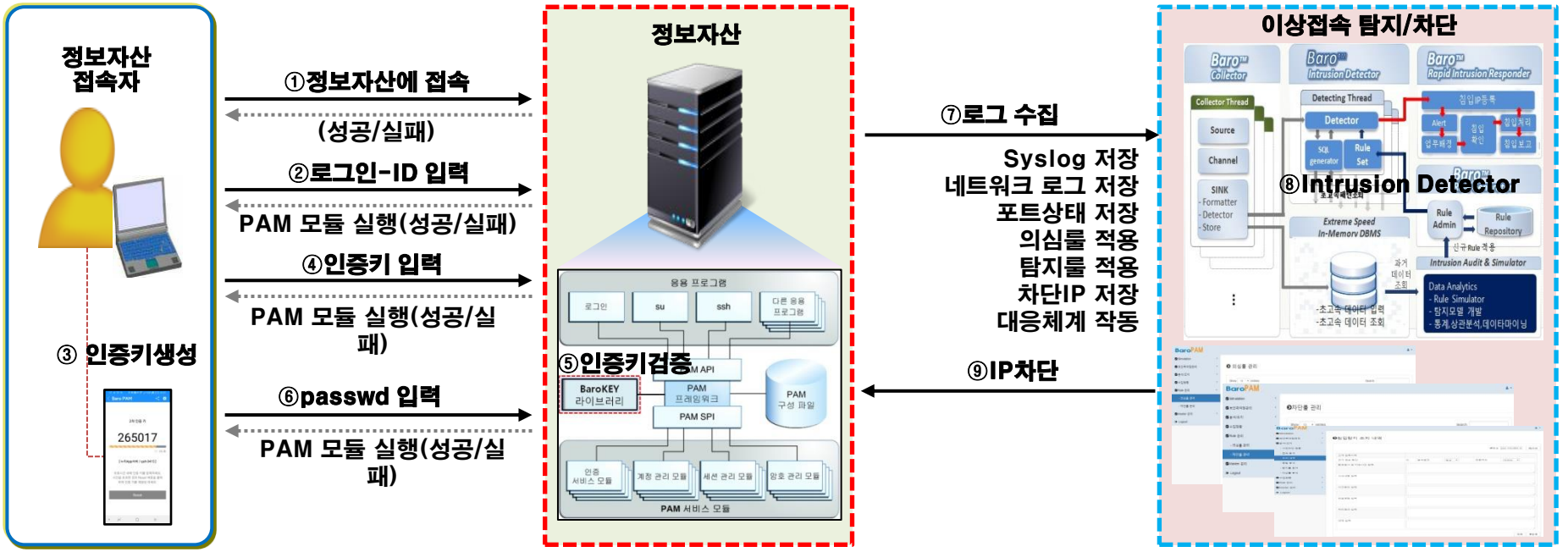


- -현장에서 검증된 탐지 및 차단 Rule 적용
- -실시간 Sys로그, 네트워크 로그, 포트상태, App로그 수집 가능
  exec, spooldir, shell, DB pooling 등
- -초고속 인메모리 아키텍쳐로 설계
- -실시간 IP차단
- -축적된 대응체계
- -Rule Audit & Simulation

5. 솔루션 시스템 FLOW

시스템 FLOW(정보자산)

BaroIDS 솔루션은 정보자산의 이상접속으로 인한 IP차단의 전체적인 시스템 Flow는 다음과 같습니다.

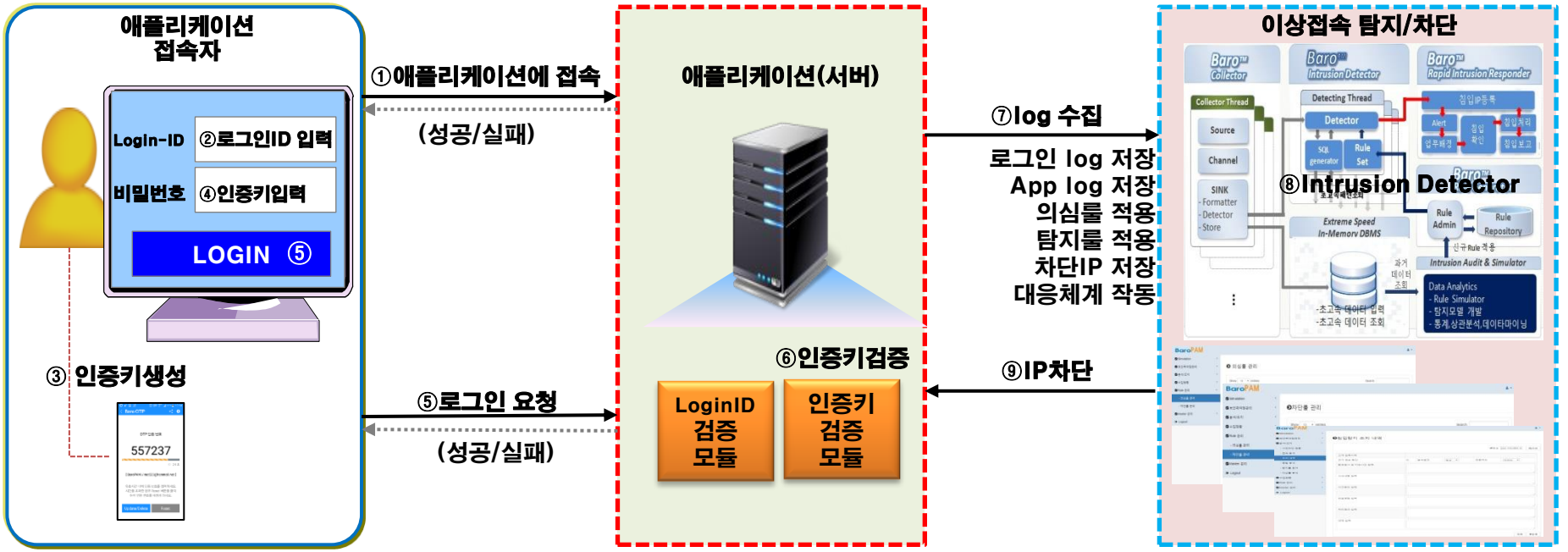


정보자산 접속 시 **일회용 인증키**를 추가 사용, **제한 시간(30초)** 및 **제한 회수(3회)**에 걸리면 자동 로그아웃 처리되며, 이상접속이 탐지가 되는 즉시 곧바로 IP가 차단됩니다.

5. 솔루션 시스템 FLOW

시스템 FLOW(애플리케이션)

BaroIDS 솔루션은 애플리케이션의 이상접속으로 인한 IP차단의 전체적인 시스템 Flow는 다음과 같습니다.



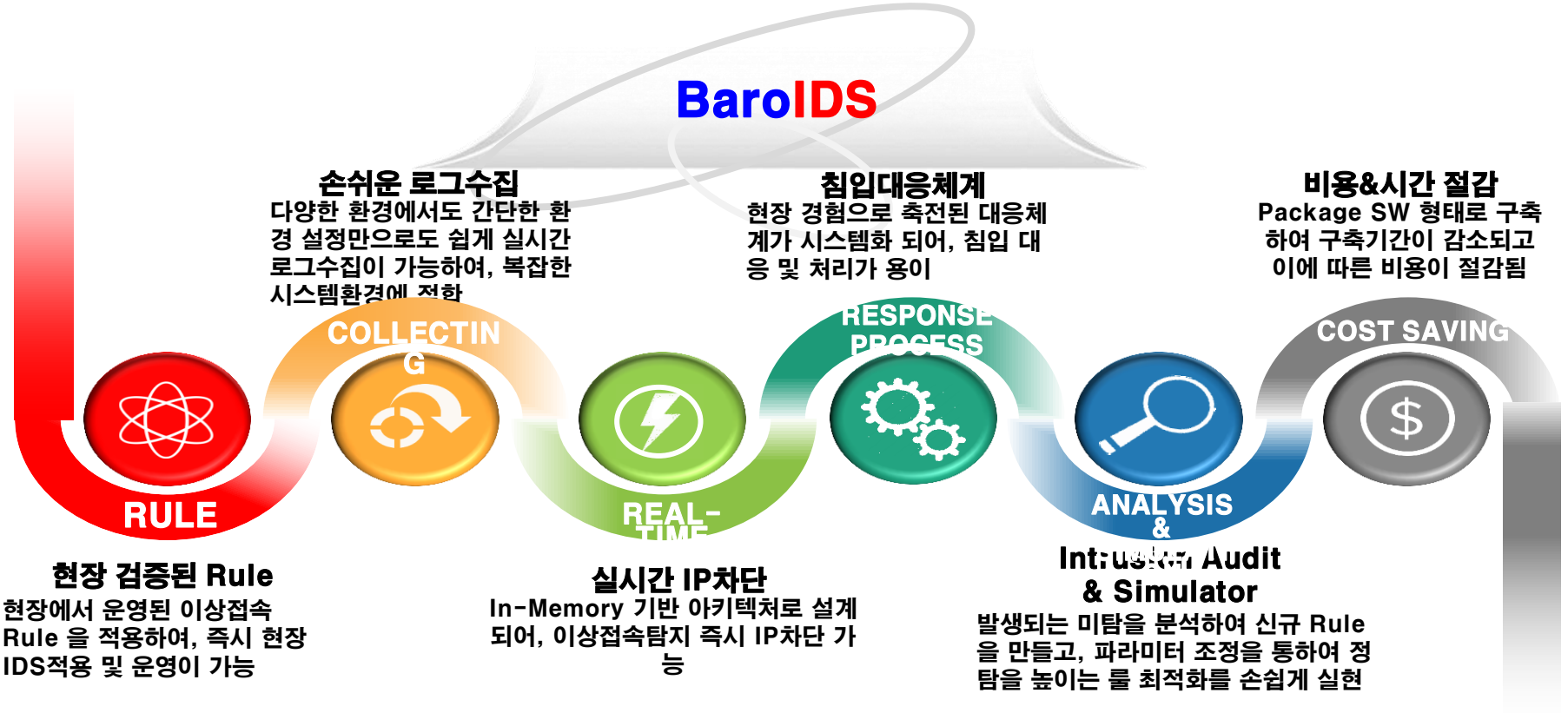
애플리케이션 로그인 시 비밀번호 대신 **일회용 인증키**를 사용하며, 이상접속이 탐지가 되는 즉시 곧바로 IP가 차단됩니다.

nurit

Why BaroIDS ?

현장에서 검증되어 개발된 솔루션으로 ① 검증된 이상접속 Rule을 보유하여, 도입즉시 성과도출이 가능하고 ② 어떠한 환경에서도 손쉽게 로그수집이 가능하며 ③ 탐지 즉시 실시간 차단이 가능하도록 초고속 인메모리 기반 아키텍처로 설계되어 있으며 ④ 사고대응프로세스를 갖추어 사고예방효과가 극대화됩니다.

이 모든 것을 짧은 구축기간과 합리적인 비용으로 구축 가능한 솔루션입니다,



7. 기타

nurit

BaroSolution 제품군

구 분	설 명	비고
BaroPAM	정보자산의 다양한 운영체제 및 애플리케이션에서 2차 인증으로 일회용 인증키를 접목시켜 중앙 집중적 인증 메커니즘을 지원하는 단순하면서도 강력한 정보자산의 접근제어 인증 솔루션.	
BaroCARD	생체정보인 지문정보를 적용한 최적의 본인인증 솔루션으로 생체정보인 지문정보를 플라스틱 카드에 등록한 후 등록된 지문정보를 인식하면 일회용 인증키를 생성하는 카드(지문인식 기능과 인증카드를 내장한 신개념 카드) 로 지문인식 인증카드 솔루션.	
BaroCRYPT	Feistel 암호를 사용하여 크기가 작고 구현이 쉬운 블록 암호화 알고리즘인 XXTEA (Extended Extended Tiny Encryption Algorithm)를 기반으로 하는 가볍고 가장 빠른 암호화 알고리즘을 적용한 솔루션.	
BaroCollector	다양한 Source에서 발생된 많은 양의 로그 데이터(Big Data)를 중앙의 데이터 저장소로 효율적으로 수집해 주는 분산처리, 신뢰성, 가용성을 갖춘 실시간 로그 수집기.	
BaroFDS	이상금융거래탐지 및 대응업무에 대한 모금융기관의 2년간의 Know-how을 바탕으로 개발된 금융권 유일의 검증된 FDS 솔루션으로서 복잡한 금융권 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있음.	
BaroIDS	정보자산(서버, 네트워크장비, 보안장비, 저장장치, 데이터베이스, 애플리케이션, 기타)의 이상접속 탐지 및 차단에 대한 현장의 Know-how을 바탕으로 FDS(Fraud Detection System)를 적용하여 개발된 솔루션.	

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 010-2771-4076