Products of Bespin Global

SecOps

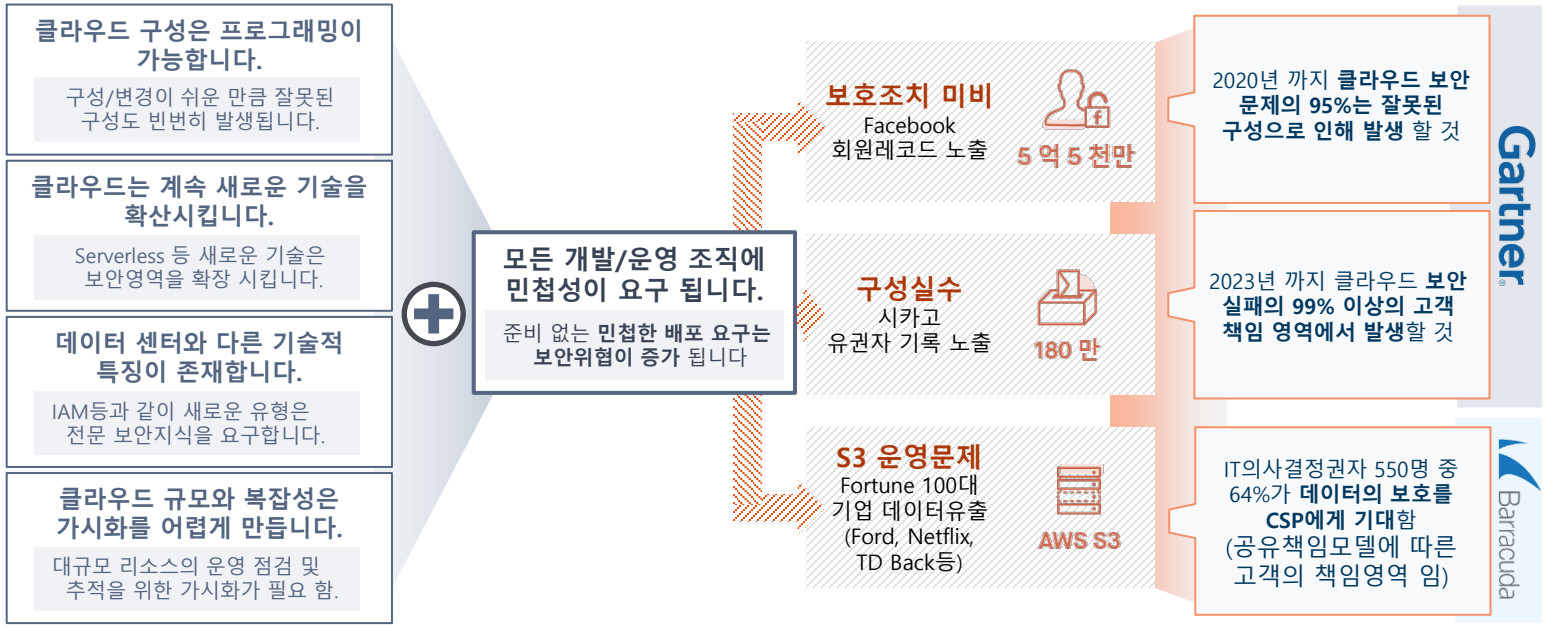
2021

BESPIN GLOBAL

HELPING YOU ADOPT CLOUD.

1. Cloud Security Consideration

Cloud에서만 제공되는 사용자 권한 및 관리형 서비스의 사용이 **증가하면서 Legacy보안 체계로는 점점 Cloud 서비스에 대한 위협을 방어할 수 없습니다.** Cloud보안을 위해서는 먼저 **Cloud의 기술특징과 위협요소를 이해**하여야 합니다.



2. Cloud Native Security의 필요성

Bespin SecOps는 기업이 운영하는 **IT서비스를 Cloud로 전환하거나 도입하는 단계에서 부터 Cloud Native환경에 이르기 까지** IT서비스를 안전하게 보호할 수 있도록 **보안계층의 설계, 구축, 운영, 관제 까지 보안 One Stop서비스를 제공**합니다.

SecOps
BESPIN GLOBAL

클라우드를 활용한 기업의 **민첩한 서비스 배포요구의 확대는** 완전한 보안체계가 없는 경우 **보안위협을 지속적으로 증가시킬 수 있습니다. 완전한 Time to Market의 요구사항에 대응** 하기 위해 **보안은 매우 중요한 요소**입니다.
Bespin SecOps는 이러한 시장의 요구에 대응하기 위해 **클라우드를 이용하는 기업이 반듯이 고려하여야 하는 6가지 주요 사항을 정의**하고, 이를 **해결하기 위한 구성된 새로운 방식의 보안서비스를 제공을 목표로** 합니다.

※ **SecOps**는 Security + Operation의 합성어로 Bespin Global이 Cloud보안을 위해 고객에게 제공하는 새로운 개념의 보안 상품입니다.

I **Cloud보안은 기술의 이해로 부터 시작됩니다.**
클라우드는 가상화 기술을 기반으로 한 새로운 기술 아키텍처 입니다. 클라우드 기술 특징에 대한 이해가 없다면 지속적이고 신뢰성 있는 보안을 구현할 수 없습니다.

II **책임공유 모델 기반의 보안정책 이 필요합니다.**
CSP가 제공하는 인프라는 데이터센터 이상의 강건함을 보장합니다. 대부분의 취약점 및 보안사고는 99% 고객의 책임영역 에서 발생하고 있음으로 고객 책임영역에 대한 이해와 대책이 필요합니다.

III **IT서비스의 특징을 고려한 보안대책을 수립 하여야 합니다.**
기업이 클라우드 환경에서 제공하는 서비스 특징 및 CSP가 제공하는 설치형 또는 다양한 관리형 서비스의 활용을 지원할 수 있는 새로운 보안솔루션의 구성과 보안정책 이 필요합니다

IV **Cloud Native 보안솔루션 및 운영기술이 필요합니다.**
Container 및 Serverless 등 새로운 관리형 컴퓨팅 서비스는 Legacy의 설치형 보안 솔루션을 이용 할 수 없음으로 Cloud Native 를 지원하는 다른 형태의 보안 솔루션이나 CSP의 보안기능에 대한 구성이 필요합니다.

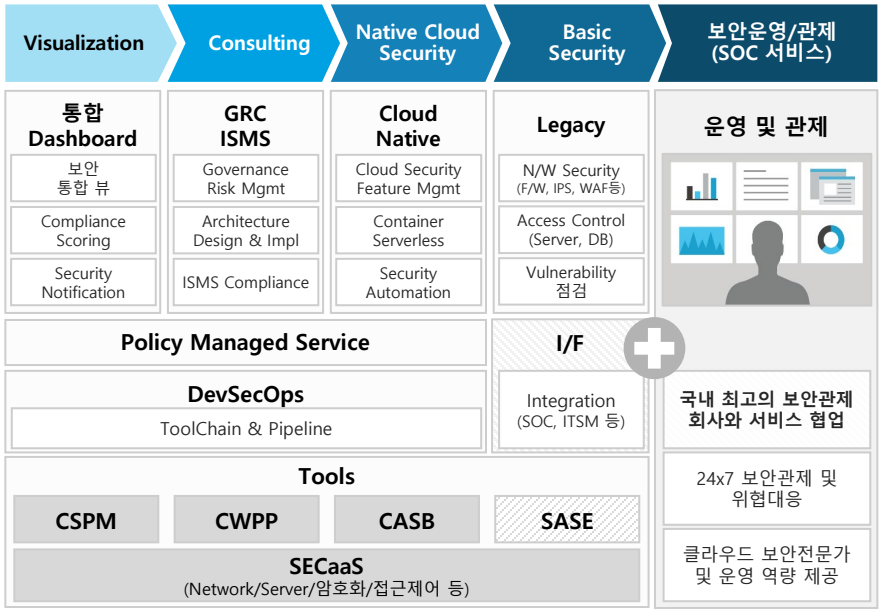
V **Cloud 보안의 점진적 자동화는 매우 중요한 항목입니다.**
클라우드에서 서비스를 개발, 배포, 운영하는 전 과정에 대한 보안 자동화가 필요합니다. DevSecOps가 목표이나 기업은 현재의 IT운영 거버넌스를 고려한 보안자동화를 구성하여야 합니다.

VI **DevSecOps로 보안영역을 Shift Left하여야 합니다.**
Security Triad (Build/Deploy/Run)의 연속된 Pipeline에서 Shift Left는 매우 중요한 원칙 이며, Shift Left를 통해 원천적으로 보안문제 를 해결 및 비용을 절감하며, 보안 부채를 지속적으로 해결 할 수 있습니다.

3. Bespin SecOps 개요

기업의 IT서비스는 Cloud를 활용한 Legacy의 단순 전환에서 새로운 컴퓨팅 환경과 **CSP**의 신 기능을 **활용한 Cloud Native**환경으로의 전환 및 확장을 요구합니다. **SecOps는 Cloud Native환경에서 필요한 새로운 보안 페러다임을 제시**합니다.

Bespin SecOps Product Landscape



Cloud Native Security No.1

4. Bespin SecOps Product 소개 (1/3)

Bespin SecOps는 Cloud 보안에서 중요한 **Consulting, Cloud Native Security, Basic Security, Integration 등 4가지 주요 보안영역과 DaaS보안 등 총 5개의 상품영역별 서비스를 제공**합니다.

상품 영역	상품 명	서비스 요약	주요 제공목록
 Consulting	Cloud Security Architecture	클라우드의 도입, 전환 및 개선이 필요한 **고객에게 보안 거버넌스 기반의 정책, 프로세스설계 및 클라우드 보안 구축 컨설팅** 서비스	• Security Assessment • To-Be Design & Planning (S) (F) + [P] [ ] [M] [O]
	Cloud Risk Assessment	클라우드 운영의 **취약점, 정책개선, Risk관리 등 을 통해 서비스 안정성을 확보**하고 **효율적인 보안 운영을 지원하는 컨설팅** 서비스	• 보안체계 분석 • Risk Management Planning (S) (F) + [P] [ ] [M] [O]
	K-ISMS Consulting	On-Prem, Private/Hybrid/Multi Cloud 등 모든 IT서비스를 운영하는 **기업의 ISMS인증을 지원하며, 정보보호관리 체계를 구축하고 유지**할 수 있도록 지원하는 **컨설팅 서비스**	• ISMS 기반 취약점 점검 • ISMS 인증지원 (S) (F) + [P] [ ] [M] [ ]
 Cloud Native Security	CSPM & CWPP Implementation (For Prisma Cloud)	**Prisma Cloud를 이용한 CSPM & CWPP구성을 지원**하고, 기업에 필요한 **관리형 Compliance 및 Policy작성/보고서/Dashboard 제공**, 솔루션 **운영에서 발생하는 각종 기술지원을 제공**합니다.	• CSPM & CWPP구성 및 지원 • Compliance 작성 및 유지 [S] [F] + [P] [I] [M] [O]
	AWS Security Feature (N/W)	AWS가 제공하는 관리형 서비스를 보호하기 위한 **Network 보호 중심의 Security Feature(Shield, WAF 등)를 구성하고 정책 및 모니터링, 위협대응을 지원**합니다.	• Feature 구성 및 정책설정 • Monitoring 및 위협대응 [S] [F] + [P] [I] [M] [ ]
	Security Automation (DevSecOps)	기업의 IT운영 거버넌스에 적합하게 구현된 **DevOps에 Security ToolChain 및 Pipeline을 추가**하여 **보안취약점의 발견 및 조치를 Shift left하고 운영상 발생하는 보안위협 보고 및 차단정책을 자동화**합니다.	• Feature 구성 및 정책설정 • Monitoring 및 위협대응 ( ) (F) + [ ] [I] [M] [ ]

범례 - License
(S) 3rd Solution
(F) CSP Feature

범례 - 제공목록
[P] Plan
[M] Monitoring
[I] Implementation
[O] Operation

4. Bespin SecOps Product 소개 (2/3)

Bespin SecOps는 Cloud 보안에서 중요한 **Consulting, Cloud Native Security, Basic Security, Integration 등 4가지 주요 보안영역과 DaaS보안 등 총 5개의 상품영역별 서비스를 제공**합니다.

상품 영역	상품 명	서비스 요약	주요 제공목록
Basic Security	Network Security	Legacy에서 전통적으로 사용되던 **FW / IPS / WAF 등 Network 기반 보안 3rd Party Solution**을 **클라우드 환경에** Agent또는 GW형태로 **배포 및 구성을 지원**하고, **보안관제를 기반으로 한 운영서비스를 제공**합니다.	• Solution Install & Config • Monitoring & Operation
	Server Security	Legacy에서 전통적으로 사용되던 **서버 보호를 위한 계정 및 접근제어, 안티바이러스 Solution**을 **클라우드 환경에** Agent또는 GW형태로 **배포 및 구성을 지원**하고, AV에 대한 **구성지원** 또는 **운영서비스**(접근제어 등)**를 제공**합니다.	• Solution Install & Config • Monitoring & Operation
	Application Security	Legacy에서 전통적으로 사용되던 **Web 서비스 보호를 위한 Web Shell을 탐지 Solution** 을 클라우드 환경에 Web서버에 Agent형태로 **배포 및 구성을 지원**하고, **Web Shell에 대한 관제 또는 운영서비스를 제공**합니다.	• Solution Install & Config • Monitoring & Operation
	Database Security	Legacy에서 전통적으로 사용되던 **DB 보호를 위한 계정 및 접근제어, 암호화 Solution**을 **클라우드 환경에** Agent또는 GW형태로 **배포 및 구성을 지원**하고, 접근제어 및 암호화에 대한 **운영서비스를 제공**합니다.	• Solution Install & Config • Monitoring & Operation
	취약점 점검	Legacy에서 전통적으로 사용되던 **웹서비스 및 네트워크 취약점 탐지를 위한 취약점 점검 Solution을 클라우드 환경에 배포 및 구성을 지원**하고, **취약점 점검 결과를 분석하고 대응 방법을 제공** 합니다.	• Architecture Plan & Impl • Monitoring & Operation
	SECaaS (보안공통존구축)	전사 **클라우드 네트워크 환경 보호**를 위한 **외부 접점 네트워크 계층에 대한 보안통제 및 제어, 취약점점검 등 보안 솔루션을 통합한 기업형 및 공유형 SECaaS 서비스** 제공	• Architecture Plan & Impl • Monitoring & Operation

범례 - License
- S: 3rd Solution
- F: CSP Feature

범례 - 제공목록
- P: Plan
- M: Monitoring
- I: Implementation
- O: Operation

4. Bespin SecOps Product 소개 (3/3)

Bespin SecOps는 Cloud 보안에서 중요한 **Consulting, Cloud Native Security, Basic Security, Integration 등 4가지 주요 보안영역과 DaaS보안 등 총 5개의 상품영역별 서비스를 제공**합니다.

아래 상품은 Bespin Global에서 준비중이며, 2021년 1Q에 출시될 예정 입니다.

범례 - License: S 3rd Solution, F CSP Feature
범례 - 제공목록: P Plan, I Implementation, M Monitoring, O Operation

상품 영역	상품 명	서비스 요약	주요 제공목록
 보안통합 Dashboard	Cloud Security Dashboard	**페르소나 별 보안 가시화 서비스**로 CISO, 보안운영자를 위해 제공되며, **표준 Bespin 표준 보안 Compliance를 기반으로 분석된 Dashboard 제공**합니다. (OpsNow에 통합 하여 제공 예정)	• Security Compliance Scoring • Custom Policy & Dashboard S + I M O
	Security Notification Service	Bespin이 제공하는 Cloud Native Security 상품 및 서비스에서 제공되는 모든 **보안 Alert 및 Incident에대한 Messaging 서비스를 제공** 합니다. (Alert Now를 통해 제공 예정)	• Security Alert Notification • Messaging Management S F + P I M O
	SoC Integration	Bespin이 제공하는 보안관제서비스 이용 시 **관제센터 모니터링에서 발생하는 모든 보안위협 메시지 및 Incident를 ITSM 등 운영 프로세스와 통합을 지원** 합니다.	• SoC Alert Message Integration • SR Integration S F + P I M O
 DaaS Security	DaaS Security	기업이 활용하는 Cloud환경의 **가상 데스크 탑 서비스에 대한 사용자계정, 사용자접근 및 권한, 접속 위치 및 원격 Device 관리 등 과 같은 보안 서비스를 제공**합니다.	• User Access Control • Remote Device Control S F + P I
	Untact Security	**기업의 재택 및 원격근무**를 위해 활용하는 **원격 데스크탑(VDI) 및 업무에 필요한 다양한 솔루션(화상, Chat, 공유파일 등)에 대한 통합 보안서비스를 제공** 합니다.	• CASB Implementation • SaaS Security Support S F + P I

5. Bespin SecOps Reference

솔루션 Partner

paloalto NETWORKS
FORTINET
TREND MICRO
Penta SECURITY
CISCO
f5
PNP SECURE
WareValley

서비스 Partner

SK infosec
AhnLab
IGLOOSECURITY
SAMSUNG 에스원

SecOps 도입 기업

SAMSUNG 삼성전자
LG전자
SK
KB국민카드
DOOSAN
한화시스템
AMOREPACIFIC
신한금융그룹
EBS
HYUNDAI

6. 고객 사례

	Challenge	정책 지원 사항
Case1 Challenge	• 멀티 클라우드 서비스에 대한 보안 Compliance 모니터링 및 관리 • 멀티 클라우드의 IAM 에 등록된 유저 및 유지보수 직원들의 권한 정리 • AWS 에 설정된 Security Group, 방화벽 취약 룰 관리 • Azure Container Service(ACS), AWS Serverless 우회 접속 관리	• 대상 Account 별 보안 컴플라이언스 위반내역 제공 • 등록 된 IAM User의 상세권한 정보 제공 • AWS SG 보안위반 사례분석 Data를 통한 정책 개선 • 컨테이너/서버리스영역의 Native 보안서비스 검토 중
Case2 Challenge	• 클라우드 서비스에 대한 보안정책 기준 부재 • IAM 에 등록된 유저 및 유지보수 직원들의 권한 및 만료 관리 • AWS 에 설정된 Security Group에 대한 만료관리	+ ISMS 정책 Custom 적용 • 클라우드 보안정책 / 가이드라인 수립 지원 • 표준 보안체크리스트 기반 정책개발/ 모니터링 자동화 • SG 사용만료 기간에 대한 Tag정보 활용 정책화 • 컨테이너& 서버리스에 대한 보안서비스 확대 검토 중

#별첨 : AWS 감사 모니터링

이벤트 로그에 대한 모니터링 정책을 수립하고 자동화 하지 않는다면 유연한 클라우드 관리 어려움

[지원 서비스 예시]

이벤트명	설명
ConsoleLogin	AWS 콘솔 로그인
CreateUser	IAM 계정 생성
DeleteUser	IAM 계정 삭제
RunInstances	VM 인스턴스 생성
StartInstances	VM 인스턴스 시작
RebootInstances	VM 인스턴스 재시작
StopInstances	VM 인스턴스 중지
TerminateInstance	VM 인스턴스 삭제
CreateBucket	S3 버킷 생성
CreateAccessKey	액세스 키 생성
UpdateAccessKey	액세스 키 활성화/비활성화
DeleteAccessKey	액세스 키 삭제
PutBucketAcl	S3 버킷 접근제어 설정
PutBucketPolicy	S3 버킷 정책 설정
AuthorizeSecurityGroupIngress	인바운드 트래픽 허용
AuthorizeSecurityGroupEgress	아웃바운드 트래픽 허용
StopLogging	CloudTrail 로깅 비활성화

#별첨 : AWS 감사 모니터링(예시)

클라우드는 상시 감사체계가 필요합니다.

잘못된 구성 → **부적절한 변경 관리** → **데이터 유출**

사용자 과실과 관련된 **'ID · 자격증명 · 키 관리'**

높은 권한을 가진 계정을 탈취하는 **'계정 도용'**

내부자 및 협력업체 직원이 악의적으로 접근하는 **'내부자 위협'**

승인되지 않은 애플리케이션**(섀도우 IT영역)**

'클라우드 서비스 **'남용과 악의적 사용'**

취약한 기능을 해킹해 파고드는 **'보안에 취약한 인터페이스와 API 사용'**

승인된 애플리케이션을 사용함에 따라 발생하는 **보안 문제**

[사용자 식별, 리소스 보호, 이상행위분석 등 보안위협 시나리오!!]

- **클라우드 관리계정에 2Factor 인증이 활성화 되어있는가?**
- **S3 등 객체 스토리지가 외부에 노출된 상태는 아닌가?**
- **S3 등 객체스토리지에 대한 접근로그가 활성화되어 있는가?**
- **클라우드 감사로그를 비활성화하려고 시도하는가?**
- **SSH나RDP등 인터넷구간에서 가상머신에 접근차단 하고있는가?**
- **VM에대해 포트스캐닝이나 SSH Brutforce등 공격이 발생하는가?**
- **다른리전에서 고비용의VM (GPU 장착등)을 생성하여 사용하는가?**

2.5 Bespin Global Cloud Security Policy Model

클라우드 보안 정책에 대한 베스핀글로벌 가이드

Bespin 클라우드ISMS-P Policy모델이란?

모델 정의

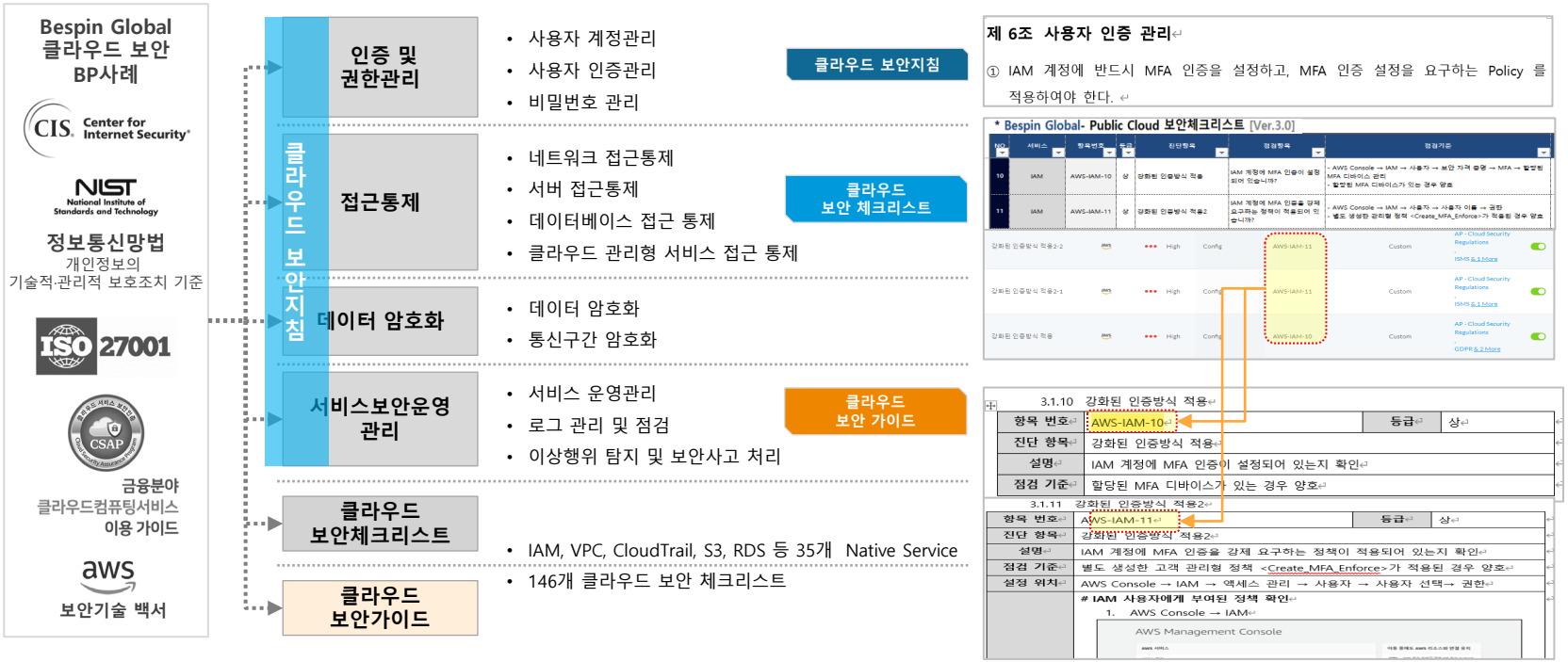
클라우드에서 사용하는 모든 서비스에 대한 보안점검 항목 / 점검기준 토대를 마련하기 위한 기준 수립이 되었으며, 이를 통한 국내 ISMS-P 등 Compliance 대응 도구

모델의 역할

국내 기업의 클라우드 도입/운영 환경에 대한 최적화 된 보안정책 제공을 목적으로 하며, 이를 통한 보안 가시성 확보 및 컴플라이언스 등 규정 준수로 보안사고 Zero化! 비즈니스 목표달성에 기여할 수 있도록 함

#별첨 Bespin Global Cloud Security Policy Model – (세부 적용 예시_1)

클라우드 보안 정책에 대한 모니터링 자동화 정책개발/반영을 통한 지속적인 보안 모니터링 가능



#별첨 : Bespin Global Cloud Security Policy Model - (세부 적용 예시_2)

Cloud보안정책 중 Prisma Only 평가항목과 수동평가 항목으로 나뉘며, 검증과정은 아래와 같음

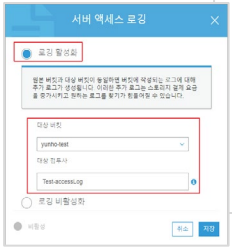
Prisma Only 판단 | 진단항목 : 서버 액세스 로깅

점검항목 : S3 버킷에 대한 서버 액세스 로깅 미 설정 대상

RQL

```
config where cloud.type = 'aws' AND
api.name='aws-s3api-get-bucket-acl' AND
json.rule='loggingConfiguration.targetBucket
equals null or loggingConfiguration.targetPrefix
equals null'
```

조치 예시 : Alert발생→ 이슈관리시스템→ 운영팀 확인/조치/ 예외



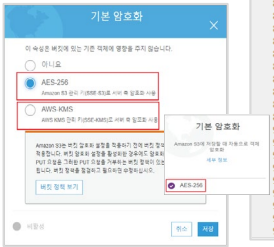
수동 평가 항목 | 진단항목 : S3 암호화

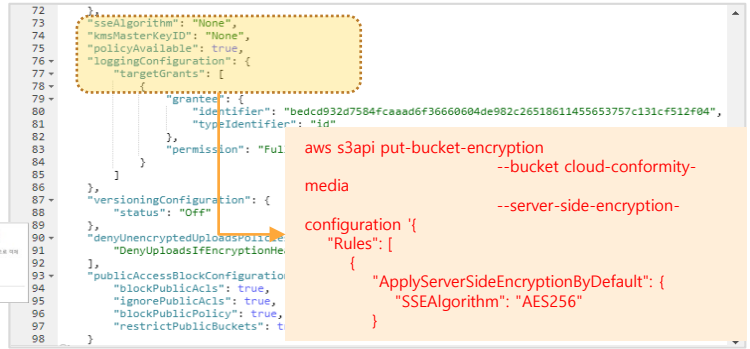
점검항목 : 개인정보가 저장되어 있는 S3 암호화 설정이 활성화 되어 있습니까?

RQL

```
config where cloud.type = 'aws' AND api.name= 'aws-
s3api-get-bucket-acl' AND json.rule = 'policyAvailable is
true and denyUnencryptedUploadsPolicies[*] is empty and
sseAlgorithm equals None'
```

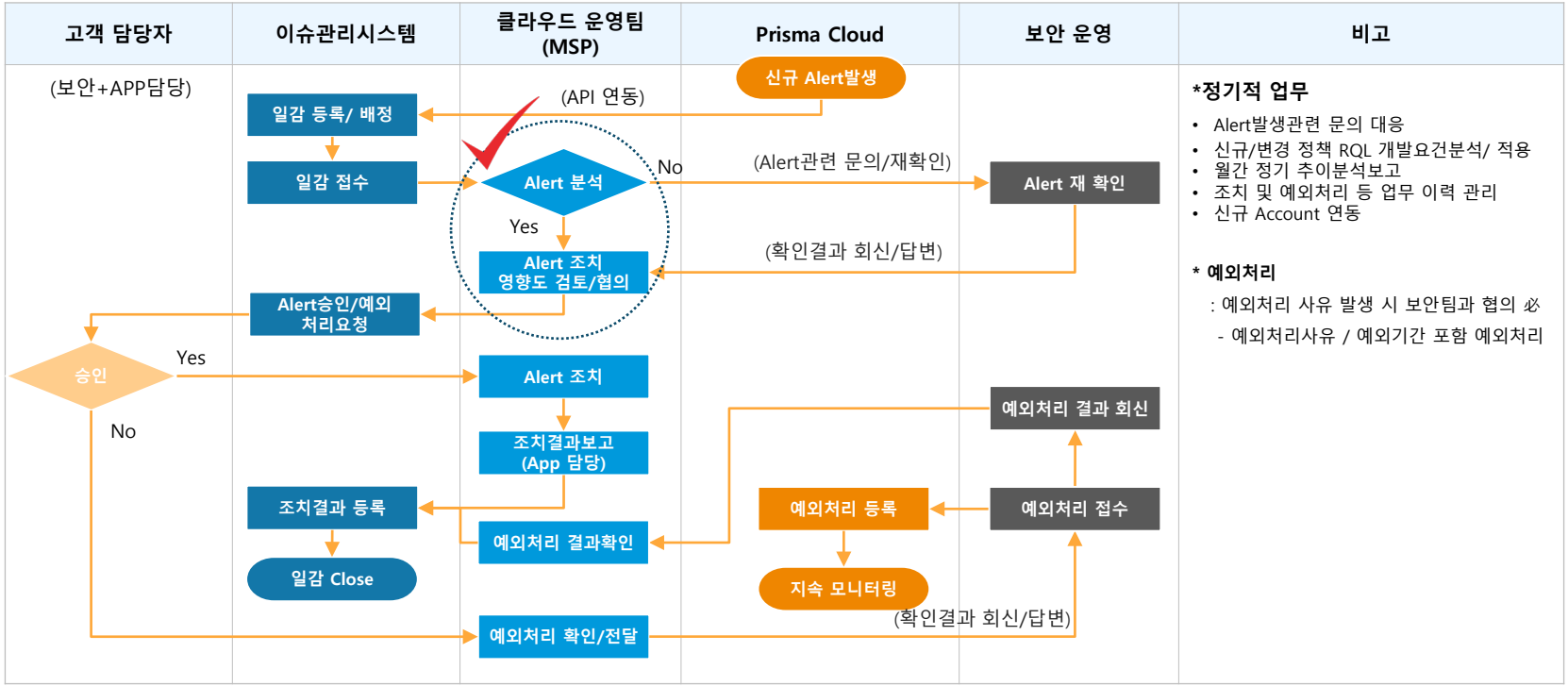
조치 예시 : Alert발생→ 이슈관리시스템→*개인정보 취급 등 중요도 검토* → 운영팀 조치/예외처리





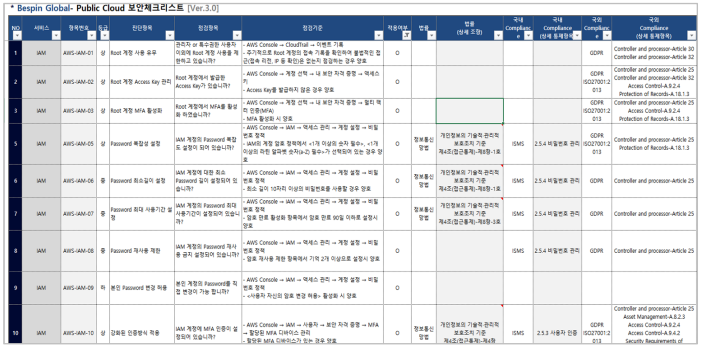
#별첨 : Bespin Global Cloud Security Policy Model - (Process Sample)

모니터링 시스템을 통해 발생된 신규 Alert 처리 프로세스는 아래와 같이 적용이 가능함



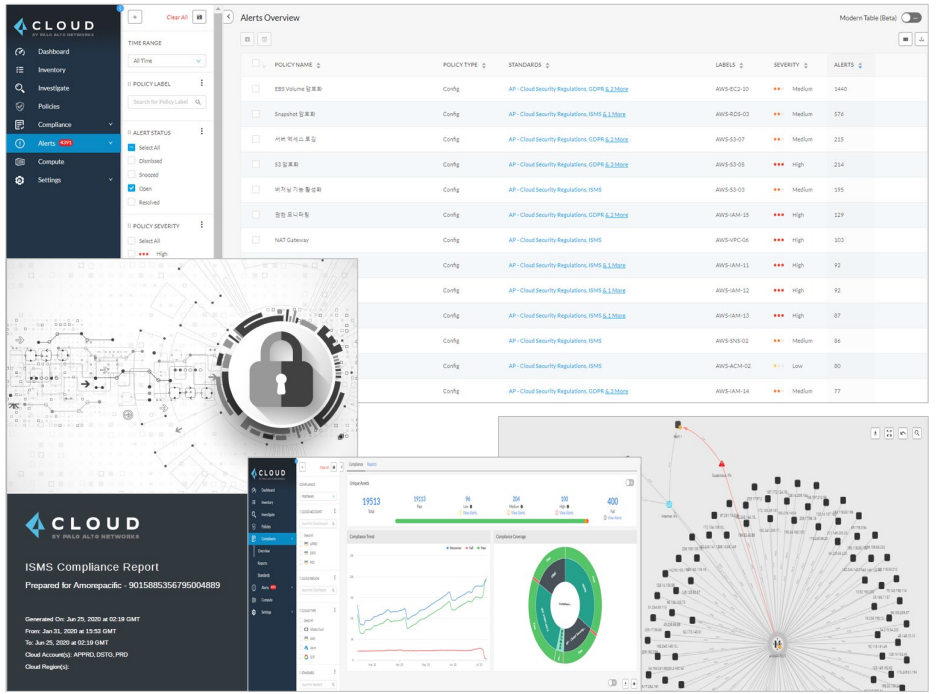
#별첨 : Bespin Global Cloud Security Policy Model - (Monitoring Sample)

클라우드 보안 정책에 대한 모니터링 자동화 정책개발/반영을 통한 지속적인 보안 모니터링 가능



• Bespin Global- Public Cloud 보안체크리스트 [Ver.3.0]

NO	서비스	정책번호	등급	진단항목	점검정책	점검기준	적용여부	법률	법률 (상세 조항)	국내 Compliance	국내 Compliance (상세 통제항목)	국외 Compliance	국외 Compliance (상세 통제항목)
1	IAM	AWS-IAM-01	상	Root 계정 사용 유무	관리자 or 특수권한 사용자 이외의 Root 계정 사용을 제한하고 있습니까?	- AWS Console → CloudTrail → 이벤트 기록 - 추가적으로 Root 계정의 접속 기록을 확인하여 불법적인 접근(접속 위치, IP 등 확인)은 없는지 점검하는 것이 양호	O					GDPR	Controller and processor-Article 30 Controller and processor-Article 32
2	IAM	AWS-IAM-02	중	Root 계정 Access Key 관리	Root 계정에서 발급한 Access Key가 있습니까?	- AWS Console → 계정 선택 → 내 보안 자격 증명 → 액세스 키 - Access Key를 발급하지 않은 것이 양호	O					GDPR ISO27001:2013	Controller and processor-Article 25 Controller and processor-Article 32 Access Control-A.9.2.4 Protection of Records-A.18.1.3
3	IAM	AWS-IAM-03	상	Root 계정 MFA 활성화	Root 계정에서 MFA를 활성화 하였습니까?	- AWS Console → 계정 선택 → 내 보안 자격 증명 → 멀티 팩터 인증(MFA) - MFA 활성화 시 양호	O					GDPR ISO27001:2013	Controller and processor-Article 25 Access Control-A.9.2.4 Protection of Records-A.18.1.3
5	IAM	AWS-IAM-05	상	Password 복잡성 설정	IAM 계정의 Password 복잡도 설정이 되어 있습니까?	- AWS Console → IAM → 액세스 관리 → 계정 설정 → 비밀번호 정책 - IAM의 계정 암호 정책에서 +1개 이상의 숫자 필수, +1개 이상의 특수 문자를 필수로 선택하여 있는 것이 양호	O	정보통신망	개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제)-제6항-1호	ISMS	2.5.4 비밀번호 관리	GDPR ISO27001:2013	Controller and processor-Article 25 Protection of Records-A.18.1.3
6	IAM	AWS-IAM-06	중	Password 최소길이 설정	IAM 계정에 대한 최소 Password 길이 설정되어 있습니까?	- AWS Console → IAM → 액세스 관리 → 계정 설정 → 비밀번호 정책 - 최소 길이 10자리 이상의 비밀번호를 사용할 것을 양호	O	정보통신망	개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제)-제6항-1호	ISMS	2.5.4 비밀번호 관리	GDPR	Controller and processor-Article 25
7	IAM	AWS-IAM-07	중	Password 최대 사용기간 설정	IAM 계정의 Password 최대 사용기간이 설정되어 있습니까?	- AWS Console → IAM → 액세스 관리 → 계정 설정 → 비밀번호 정책 - 암호 만료 활성화 항목에서 암호 만료 90일 이하로 설정시 양호	O	정보통신망	개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제)-제6항-1호	ISMS	2.5.4 비밀번호 관리	GDPR	Controller and processor-Article 25
8	IAM	AWS-IAM-08	중	Password 재사용 제한	IAM 계정의 Password 재사용 금지 설정되어 있습니까?	- AWS Console → IAM → 액세스 관리 → 계정 설정 → 비밀번호 정책 - 암호 재사용 제한 항목에서 기억 2개 이상으로 설정시 양호	O			ISMS	2.5.4 비밀번호 관리	GDPR	Controller and processor-Article 25
9	IAM	AWS-IAM-09	하	본인 Password 변경 적용	본인 계정의 Password를 직접 변경이 가능 합니까?	- AWS Console → IAM → 액세스 관리 → 계정 설정 → 비밀번호 정책 - 사용자 자신의 암호 변경 허용> 활성화 시 양호	O						
10	IAM	AWS-IAM-10	상	강화된 인증방식 적용	IAM 계정에 MFA 인증이 설정되어 있습니까?	- AWS Console → IAM → 사용자 → 보안 자격 증명 → MFA 할당된 MFA 디바이스 관리 - 할당된 MFA 디바이스가 있는 것이 양호	O	정보통신망	개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제)-제6항	ISMS	2.5.3 사용자 인증	GDPR ISO27001:2013	Controller and processor-Article 25 Asset Management-A.8.2.3 Access Control-A.9.2.4 Access Control-A.9.4.2 Security Requirements of



2.6 Bespin Compliance Value Point!

Bespin
Value Point!

내/외부 **보안 Hole 제거**	- 클라우드 운영환경에 대한 **보안향상** - 잠재적인 외부 해킹시도에 따른 Risk 제거 및 **지속 모니터링을 통한 위협 대응**
Cloud 보안정책	- Bespin 클라우드 보안정책/ 기준을 통한 **사용자(고객사)보안정책 기준 최적화** - 클라우드 Business 대하여 효과적으로 L/H/C 할 수 있는 기반 마련 - 클라우드 환경의 ISMS 심사대응 및 국제 Compliance 규제 대응 용이
지속적인 **모니터링 자동화**	- 다양한 Integration을 통한 **운영절차 간소화/ 자동화 방안 제공** - 클라우드 환경에 대한 보안 가시성 확보 및 **기준에 대한 보안 준수율 상시제고** - 지속적 모니터링을 통한 **구성오류 Zero化 및 외부 공격에 대한 일차 방역체계 마련** - 내/ 외부 환경변화 RQL을 통한 개발/반영하여 효과적인 운영 기대
클라우드 보안 **확장성**	- 멀티 클라우드(AWS, Azure, GCP, Ali) 확대 시 **동일한 수준의 보안관리 가능** - 클라우드 Native서비스 (Serverless, 컨테이너 etc.) 보안통제 등 확대 가능

Products of Bespin Global

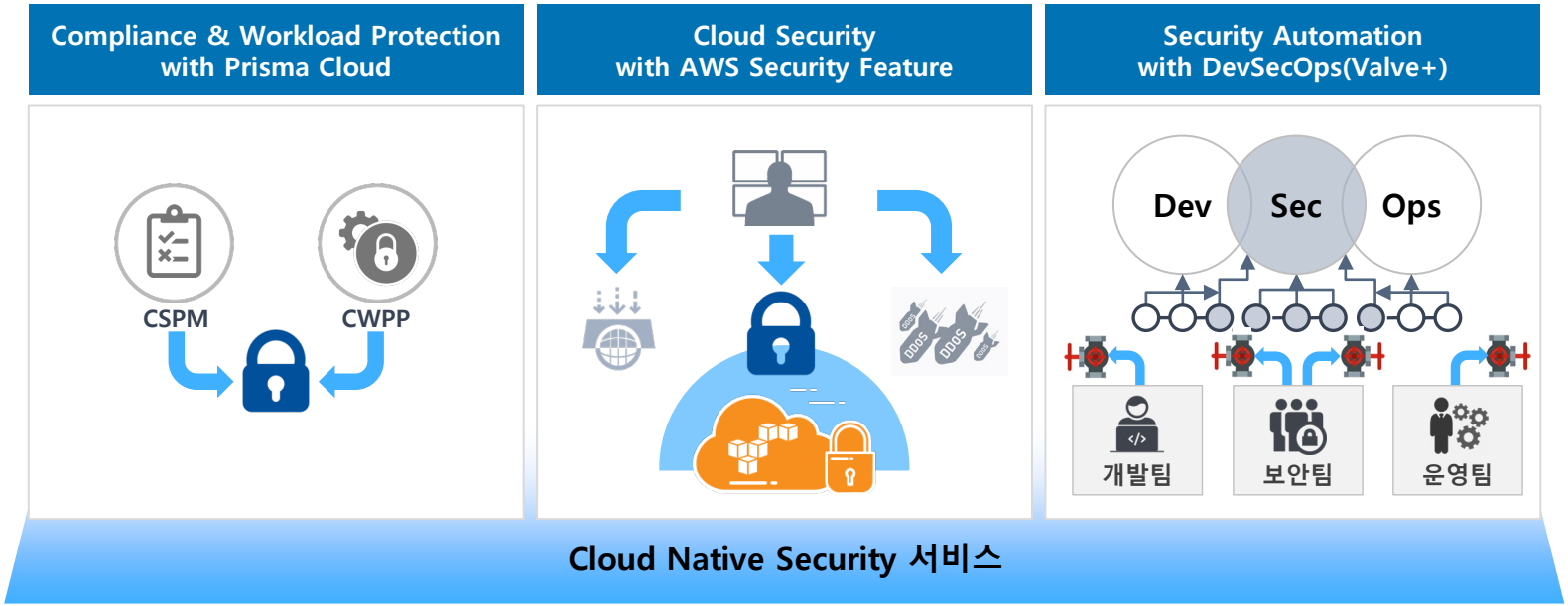
Bespin
Cloud Native Security

BESPIN GLOBAL

HELPING YOU ADOPT CLOUD.

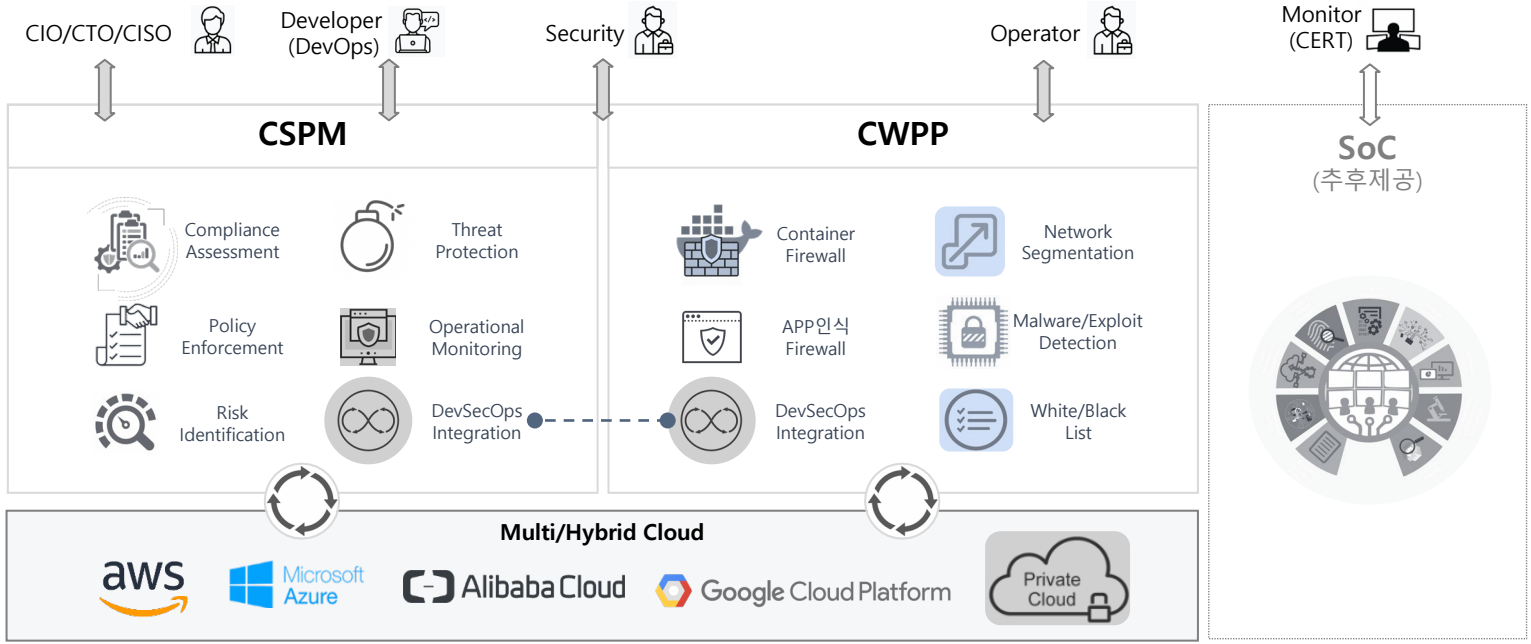
1. Cloud Native Security 상품 개요

Cloud Native 환경에서는 Traditional IT 보안서비스 및 솔루션만으로 대응할 수 없습니다. Bespin은 CSPM, CWPP영역, 클라우드 공급자가 제공하는 보안 Feature영역 및 자동화 Pipeline을 통해 완벽한 Cloud Native Security서비스를 제공합니다.



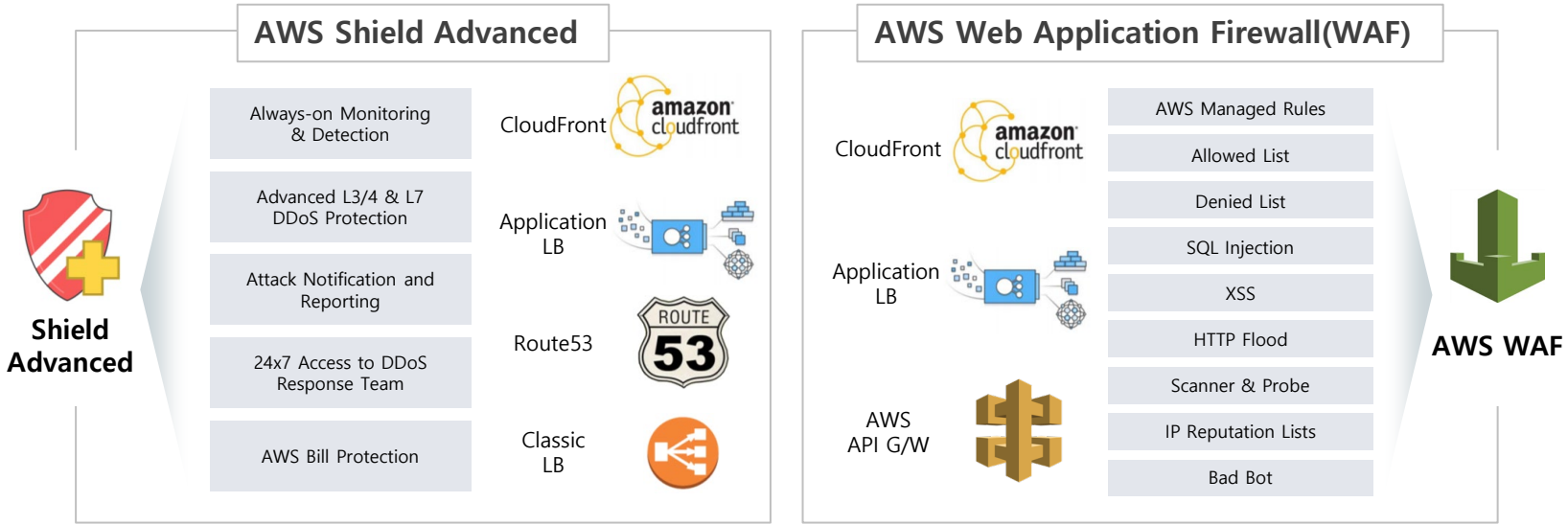
1.1 CSPM & CWPP with Prisma Cloud

Cloud Native 환경에서는 인프라 자산 및 구성, 서비스의 배포가 필요에 따라 신속하게 적용 되어야 함으로 표준 Compliance, 모범사례 및 원천적인 취약점 점검이 매우 중요하며, 새로운 기술인프라에 대한 보호가 필요합니다.



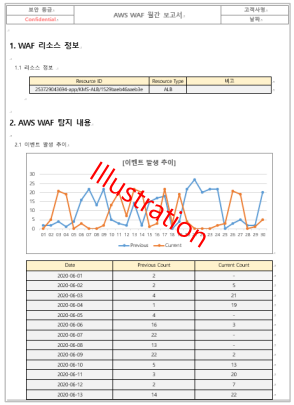
1.2 Cloud Security with AWS Security Feature

AWS Cloud 환경에서 DDoS 및 Cloud Native Application의 외부 위협에 대한 보호가 필요하며, Bespin Global은 Shield, WAF등 AWS Security Feature를 활용한 Network방어기능을 구성하고 운영/관리하기 위한 최적의 서비스를 제공합니다.

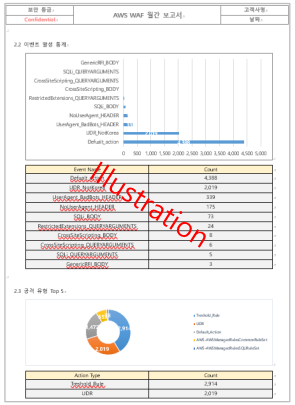


별첨 : Cloud Security with AWS Security Feature : WAF 보고서(월) Sample

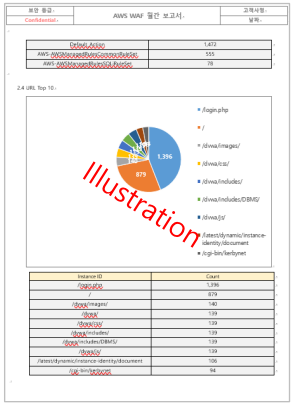
WAF리소스 및 탐지



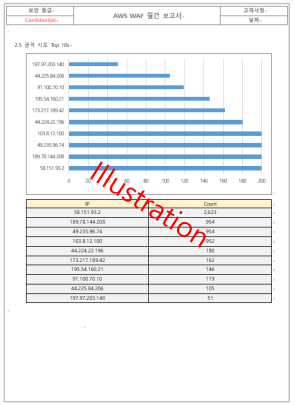
이벤트 및 공격 유형



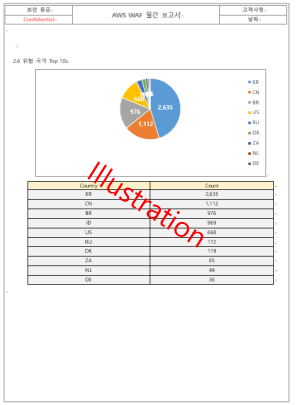
URL Top 10



공격 시도 Top 10

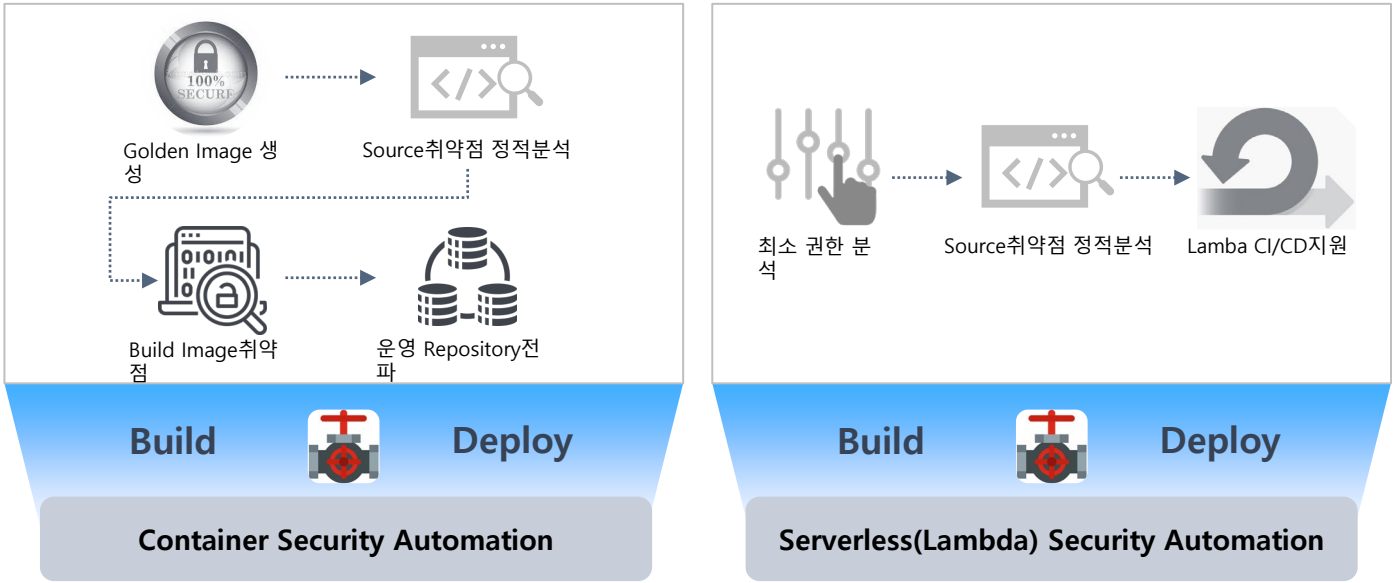


위험 국가 Top 10



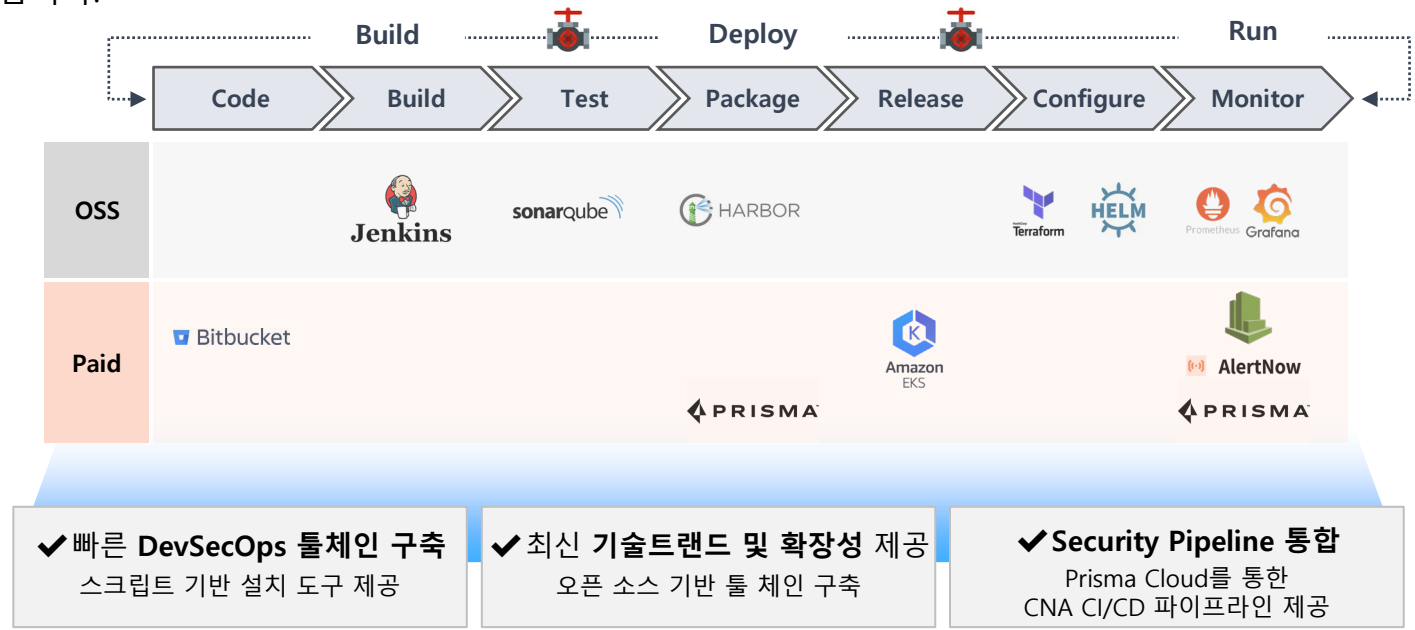
1.3 Security Automation with Container/Serverless (1/2)

Security Automation Pipeline을 기업의 운영 거버넌스 및 DevOps성숙도에 따라 순차적으로 보안영역을 도입할 수 있도록 구성한 Security Automation상품과 개발/운영/보안을 One-Team에서 운영할 수 있는 DevSecOps상품을 제공합니다.



1.3 Security Automation with DevSecOps (2/2)

Security Automation Pipeline을 기업의 운영 거버넌스 및 DevOps성숙도에 따라 순차적으로 보안영역을 도입할 수 있도록 구성한 Security Automation상품과 개발/운영/보안을 One-Team에서 운영할 수 있는 DevSecOps상품을 제공합니다.



Thank You