클라우드로의 전환과 보안 대응 방안

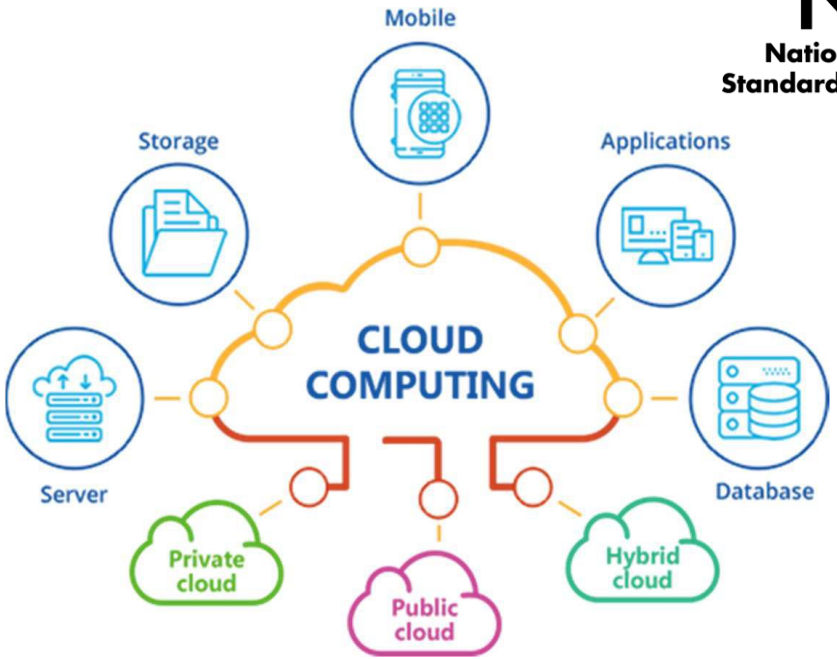
CNAPP

엔시큐어(주) 박정만 이사/본부장

eNsecure
엔시큐어㈜

급변하는 비즈니스 환경과 서비스를 보호하는 방안

Cloud 컴퓨팅의 사전적 정의



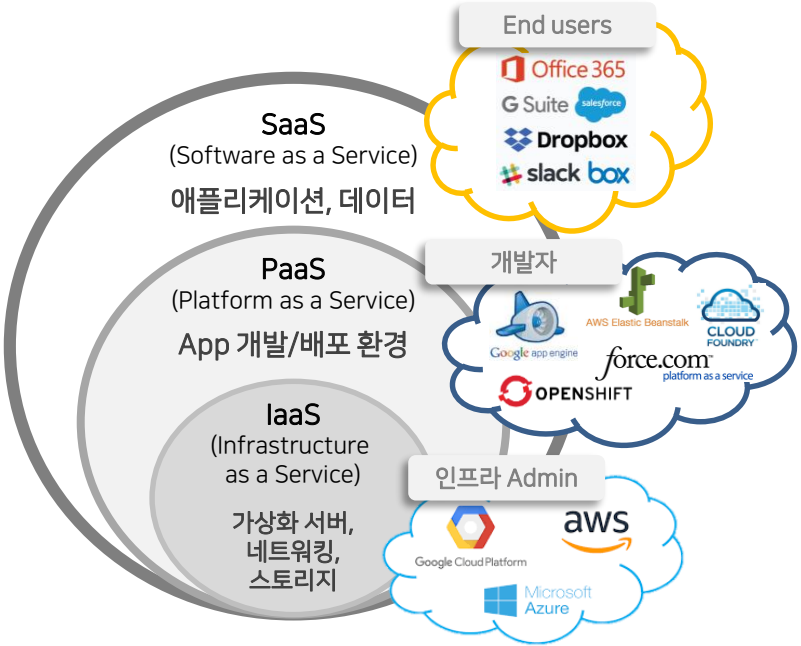
NIST
National Institute of
Standards and Technology

클라우드 컴퓨팅이란
네트워크, 서버, 스토리지, 애플리케이션, 서비스 등의
컴퓨팅 리소스에 언제든지 편하게 접근할 수 있는 기술

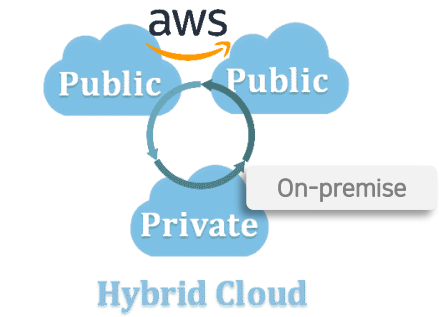
핵심은
'소유'에서 '사용'으로의 패러다임 전환

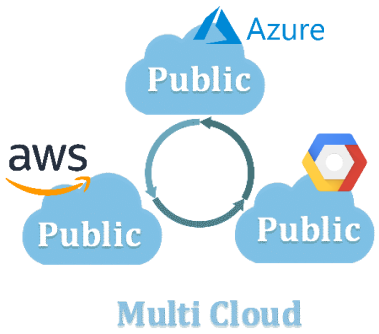
Cloud 컴퓨팅의 분류

서비스 제공 범위에 따른 구분

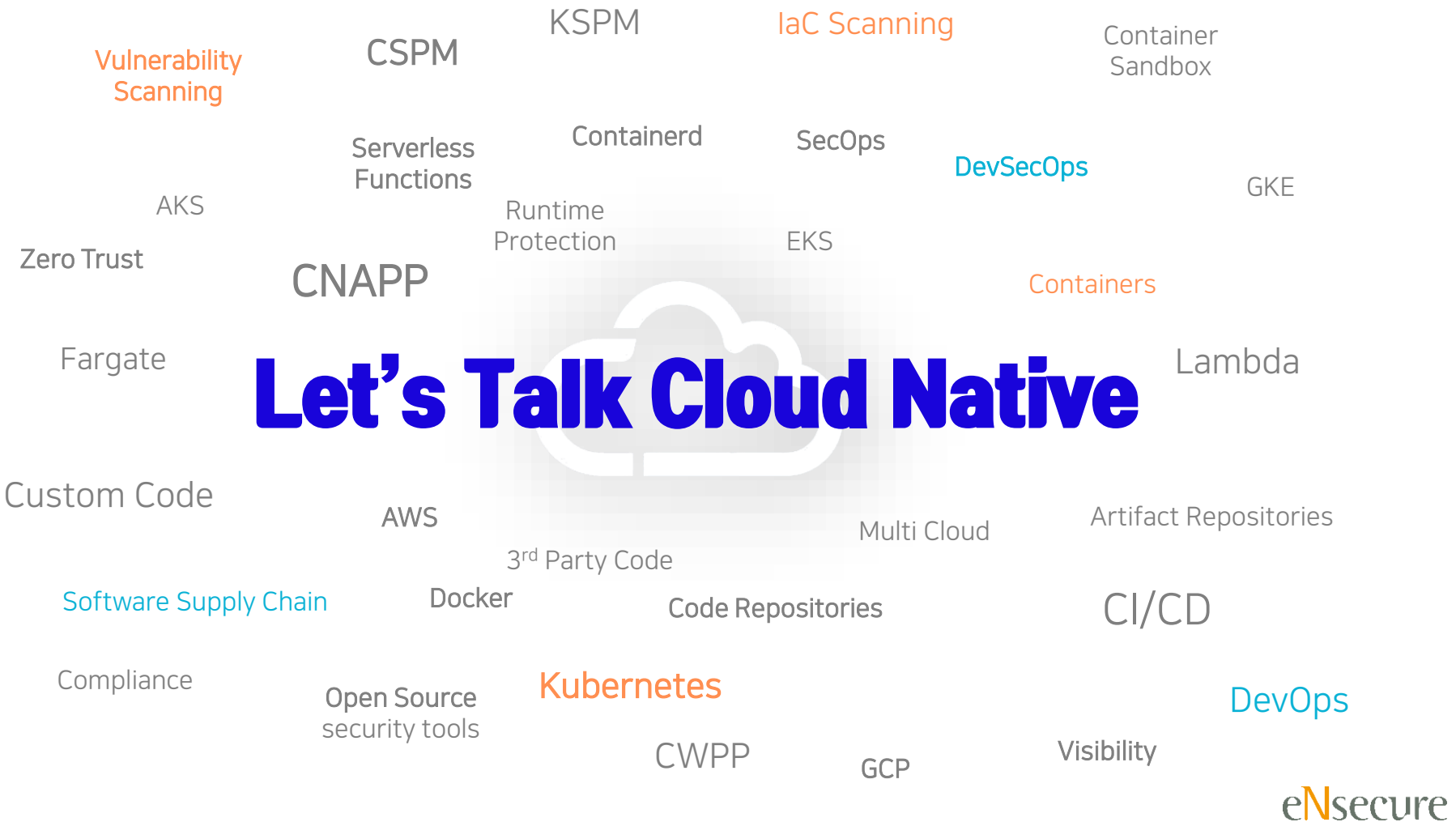


서비스 사용 형태에 따른 구분





eNsecure


KSPM
IaC Scanning
Container Sandbox
Vulnerability Scanning
CSPM
Containerd
SecOps
Serverless Functions
DevSecOps
GKE
AKS
Runtime Protection
EKS
Zero Trust
CNAPP
Containers
Fargate
Let's Talk Cloud Native
Lambda
Custom Code
AWS
Multi Cloud
Artifact Repositories
3rd Party Code
Software Supply Chain
Docker
Code Repositories
CI/CD
Compliance
Kubernetes
DevOps
Open Source security tools
CWPP
GCP
Visibility
eNsecure

Cloud Native 앱 개발은 전환점에 와 있습니다.

Gartner

개발부서의

51%

Cloud Native 환경 사용

2025년까지

95%

클라우드 네이티브로
비즈니스 인프라 전환 계획 보유

Traditional tools are not effective

레거시 보안도구는 클라우드 네이티브 환경에서 효과적이지 않습니다.

49%

사이버공격 중 클라우드 서비스를 타깃한 공격의 비율

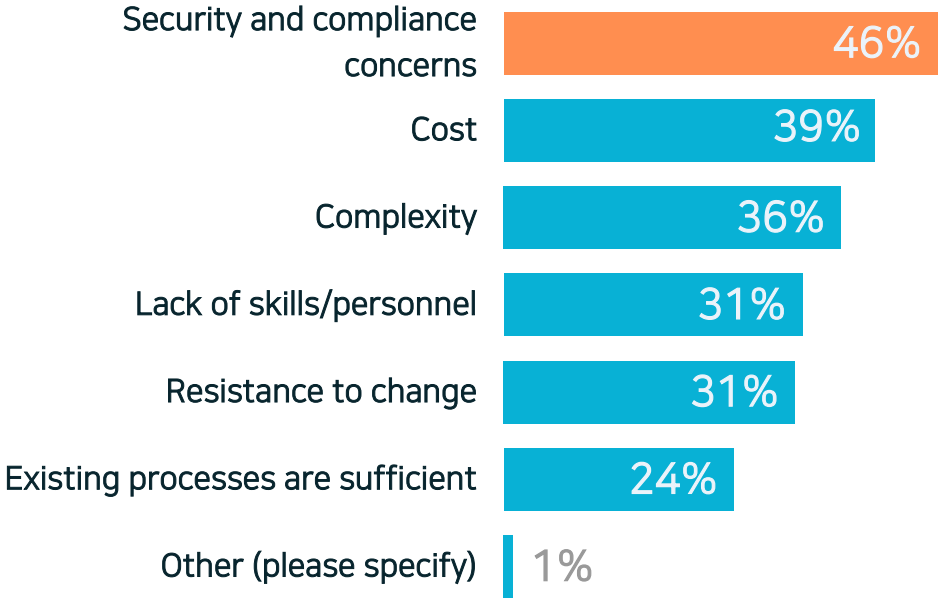
20 Minutes

log4j 가 취약한 클라우드 네이티브 워크로드를 손상시키는데 걸리는 시간

*DoK Community Report, Sep 2021
**"Cloud Will be the Centerpiece of New Digital Experiences", Gartner, Nov. 10, 2021
***Team Nautilus research

eNsecure

보안은 클라우드 도입을 위한 최고의 도전과제입니다.



451 Research
451 Research Business Impact Report

eNsecure

클라우드 네이티브 공격에 대한 위험 관리 방안

Asset

Cloud Native Business 의 생성, 저장, 배포, 운영의 전 과정의 가시성 확보 및 위험 관리를 수행해야 합니다.

- Asset and risk visibility
- Risk reduction with assurance
- Runtime visibility
- Runtime enforcement

가트너가 설명하는 하는 CNAPP

"클라우드 네이티브 애플리케이션의 최적의 보안을 위해서는 개발 단계에서 시작하여 런타임 보호로 확장되는 통합적인 보안 접근 방식이 필요합니다."

"보안 리더는 보안을 위한 통합 생명 주기 접근 방식을 제공하는 새로운 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)을 고려해야 합니다. "

Gartner

*Source: Gartner, Innovation Insight for Cloud Native Protection Platforms, 25 August 2021

The Cloud Native Application Protection Platform (CNAPP)

Dev	DevOps/DevSecOps	Engineering/SRE/Cloud Architect	Security Operations
Trust your Code		**Harden your Infrastructure**	**Protect your Workloads**
argon an aqua company Vulnerability Scanning CI/CD Supply Chain Security		Categorization Orchestrator Compliance	Container / VMs / Server Protection
		CSPM KSPM	CWPP
aqua trivy, aqua tfsec, aqua cloudsploit		aqua kube-hunter, aqua kube-bench, aqua starboard	aqua tracee

Open Source Innovation
Cloud Security Insights
Behavioral Indicators

aqua

Front Line Research
Ecosystem Integrations
Compliance

모든 서비스 구간에서 클라우드 네이티브 공격 차단

Detect, prioritize and reduce risk

코드에서 프로덕션까지 규정 준수 보장

Protect the supply chain

클라우드 네이티브 공격이
발생하기 전에 방지

Stop attacks, not your business

워크로드를 중단하지 않고
프로덕션의 불변성 제공

Reduce noise, save time

A single unified platform for cloud native application protection

eNsecure
엔시큐어㈜

아쿠아의 워크로드 보호를 이용한 런타임 보호

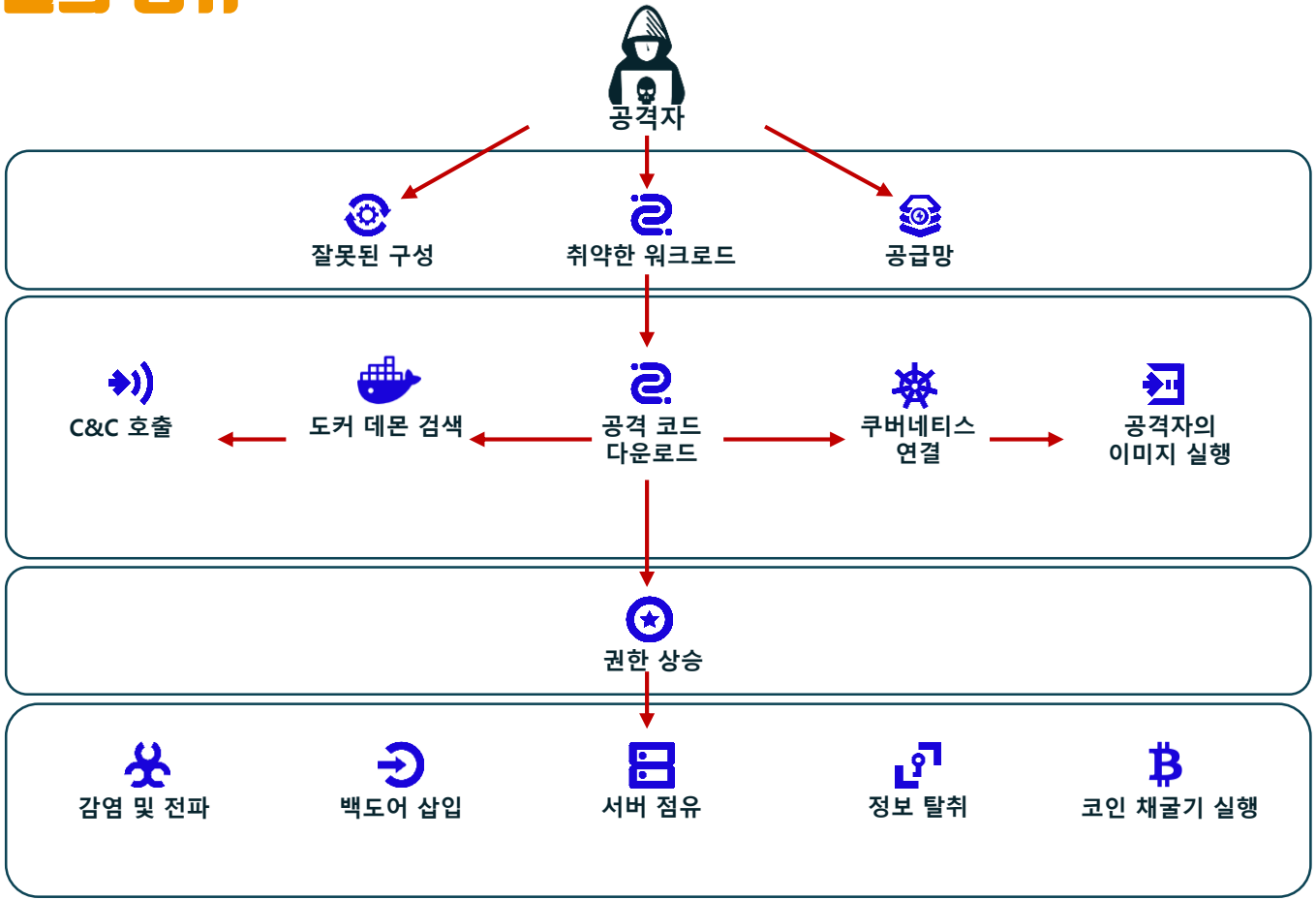
기업 대상의 공급망 공격의 증가

- 랩서스는 처음 모습을 드러낸 이후 1년도 안되는 시간동안 글로벌 기업들을 연이어 해킹하며 기업들의 데이터를 유출 했습니다.
- 그들의 공격은 크리덴셜 탈취, 시스템 접근 권한 확보, 권한 상승, 데이터 유출로 취약점을 이용한 공격 기법을 사용하였습니다.

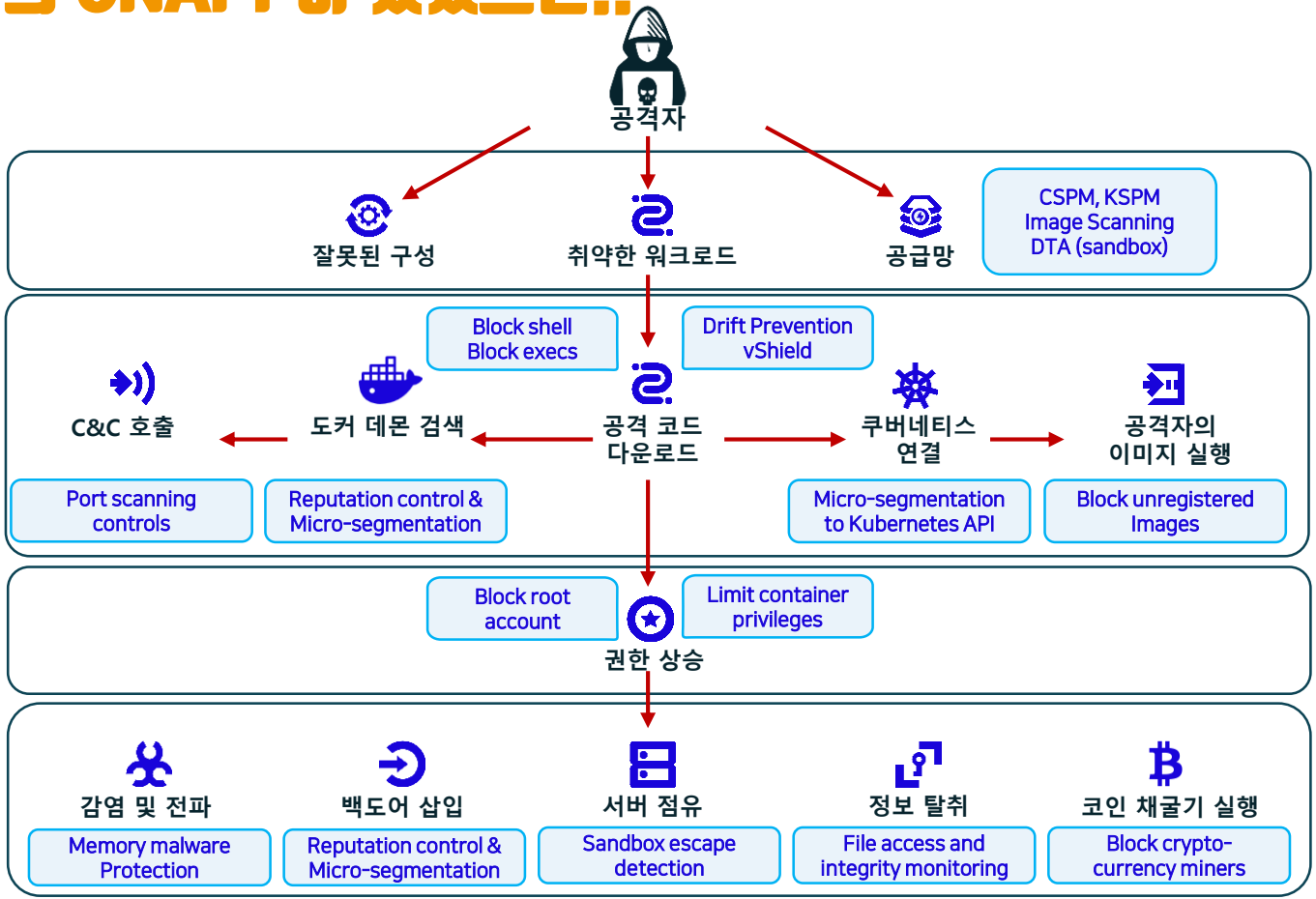
LAPSUS$ 공격 타임라인

"서비스 전 구간에서 위험 요소를 식별하고 대응· 관리 하는 것만이 위험을 예방할 수 있습니다"

공격자들의 행위


공격자
잘못된 구성
취약한 워크로드
공급망
C&C 호출
도커 데몬 검색
공격 코드 다운로드
쿠버네티스 연결
공격자의 이미지 실행
권한 상승
감염 및 전파
백도어 삽입
서버 점유
정보 탈취
코인 채굴기 실행

아쿠아의 CNAPP이 있었으면..



eNsecure

eNsecure
엔시큐어㈜

We stop cloud native attacks

엔시큐어 부스 소개

eNgen AUNES

Real-time Auto Network System
실시간 장애 예측·진단 시스템

- 실시간 네트워크 가시성 확보 및 장애 예측
- 트래픽 병목현상·장애·지연 상황 선제 대응
- 10Gbps 이상의 대용량 패킷 분석 지원
- 고 위험군 장애 발생 가능성 파악 및 관리
- 장비 성능 저하 원인의 상관관계 분석

eNsecure

Thank you

eNsecure
엔시큐어㈜