클라우드 환경의

침해사고 분석

BCGLAB 보안 연구실 - 최홍석

개요

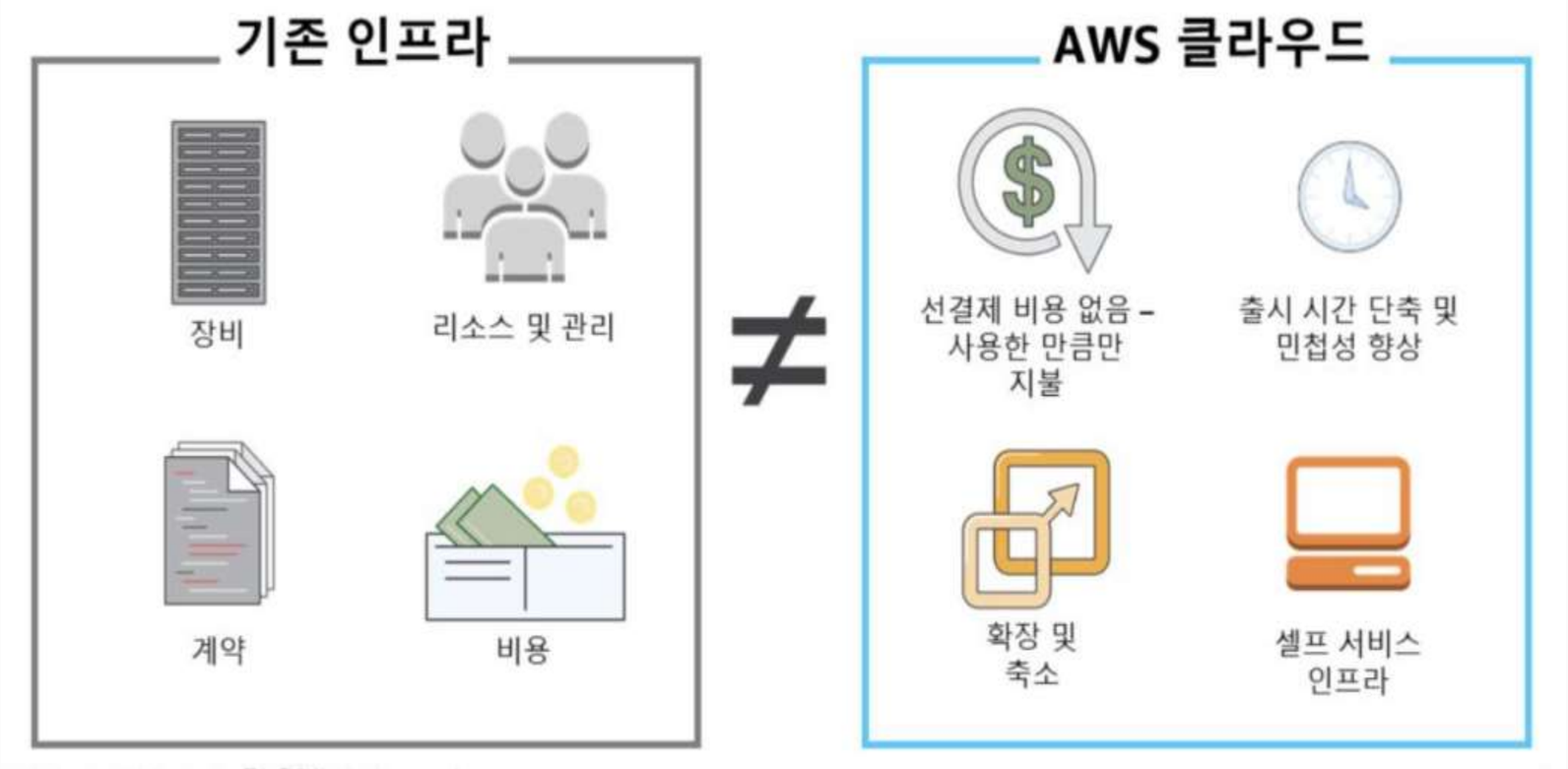
클라우드 환경의 침해사고 분석

- 코로나19로 인한 경기침체와 국내•외 비즈니스 환경의 불안정성은 산업전반에 영향
- 비대면 수요 급증이 디지털 전환의 가속화를 이끌면서 경제•사회 구조의 대전환을 맞이하게 되었고, 디지털전환의 패러다임은 유연한 비즈니스 운영을 위한 IT인프라 운영방식에도 영향
- 기업이 서버를 자체적으로 보유하고 직접 설치 및 운영하는 방식인 온프레미스환경에서 벗어나, 필요한 만큼 즉시 사용 가능한 자원에 대한 비용을 지불하는 클라우드 전환이 가속화

개요

클라우드 환경의 침해사고 분석

- 온프레미스 환경에서 클라우드 환경으로의 전환 이유는 크게 편의성, 유연성, 경제성
- 클라우드 서비스 환경은 온프레미스 환경과 달리 정보자산을 구축하기 위한 물리적 설치 공간이 필요X
- 클라우드 환경은 정보자산 운영에 필요한 시간에만 구동되므로 불필요한 비용이 소요↓(불필요한 자원의 낭비를 최소화하고 비용↓)



개요

클라우드 환경의 침해사고 분석

- 2018년 11월에는 AWS에 서울 지역에서 EC2 인스턴스가 내부 DNS 서버 설정 오류로 인하여 84분간 DNS 기능을 사용할 수 없는 사고가 발생

- 2019년 미국의 대형 은행인 Capital One에서는 AWS에 저장된 고객 개인정보 유출 사고가 발생

클라우드 서비스의 공유 책임 모델

클라우드 환경의 침해사고 분석

- 클라우드 서비스 배포 모델은 퍼블릭 클라우드, 커뮤니티 클라우드, 프라이빗 클라우드, 하이브리드 클라우드
- 클라우드 서비스 모델은 IaaS, PaaS, SaaS로 나뉠 수 있으며, 사용자가 서버를 직접 관리할 필요가 없는 서버리스모델인 FaaS와 BaaS서비스 모델도 존재
- 사용자가 관리해야 하는 자원이 많은 서비스 유형은 IaaS
(OS, 미들웨어, 애플리케이션 및 데이터와 같은 자원들을 관리)
- 클라우드 제공업체가 관리 해야 하는 자원이 가장 많은 서비스 유형은 SaaS(제공업체는 클라우드 서비스에서 제공하고 있는 다수의 서비스에 대하여 관리주체가 됨)

구분		IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
특징		확장성 높고 자동화된 컴퓨팅 리소스를 가상화하여 제공 고객에게 서버, 네트워크, OS, 스토리지를 가상화하여 제공하고 관리	서비스는 주로 응용 프로그램을 개발할 때 필요한 플랫폼을 제공 고객에게 OS, 미들웨어, 런타임과 같은 소프트웨어 작성을 위한 플랫폼을 가상화하여 제공하고 관리	사용자에게 제공되는 소프트웨어를 가상화하여 제공 고객을 대신하여 소프트웨어와 데이터를 제공하고 관리
관리 주체	제공 업체	서버, 네트워킹, 가상화 및 스토리지를 관리	서버, 네트워킹, 가상화 및 스토리지, OS, 미들웨어와 같은 자원 관리	서버, 네트워킹, 가상화 및 스토리지 뿐만 아니라 OS, 미들웨어, 애플리케이션 및 데이터와 같은 자원 관리
	사용자	OS, 미들웨어, 애플리케이션 및 데이터와 같은 자원들을 관리	데이터, 애플리케이션 관리	-

클라우드 서비스는 사용자가 원하는 서비스 유형을 선택하고,
제공자가 어떤 서비스 모델을 제공하는지에 따라 서비스 배포 모델과 서비스 모델로 구분

클라우드 보안 인증 제도

클라우드 환경의 침해사고 분석

- 클라우드 보안 인증제도는 국제 인증제도와 국내 인증제도가 존재
- 국내에는 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하는 클라우드 보안인증제가 있음
- 해당 인증기준은 IaaS 인증과 SaaS 표준등급, SaaS 간편등급 인증에 따라 각 통제항목으로 구성

구분	적용 대상	특징
클라우드 서비스 보안 인증제 (CSAP)	클라우드 서비스 제공자 (IaaS, SaaS)	공공기관에 클라우드 서비스를 제공하고자 하는 민간 클라우드 사업자는 의무 금융분야 클라우드 서비스 자체 평가 시 '클라우드 서비스 보안 인증제 항목 + 금융부문 추가 보호 조치' 적용 서비스 유형에 따른 통제항목 구성 -IaaS 인증: 14개 분야 117개 항목 -SaaS 표준등급 : 13개 분야, 78개 항목 -SaaS 간편등급 : 11개분야, 30개 항목

클라우드 보안 인증 제도

클라우드 환경의 침해사고 분석

- 국제 인증제도들은 국내의 인증제도인 클라우드 보안인증제와 다르게 클라우드 서비스 제공업체뿐만 아니라 이용자가 적용 대상에 포함되는 것이 특징
- 클라우드 보안 인증제도는 기업의 정보보호 활동을 체계적으로 수행할 수 있도록 하며 정보보호 사고를 예방하고 피해를 최소화
- 하지만 이러한 인증제도를 도입하지 않거나 일부 분만 규정하고 사용할 경우, 사용자가 아무리 조심하고 예방하더라도 보안사고는 발생

구분	적용 대상	특징
ISO 27017	클라우드 서비스 제공자 및 이용자 (IaaS, PaaS, SaaS)	클라우드 정보보호를 위해 ISO 27002에 클라우드 서비스에 특화된 구현 지침과 통제 항목 7가지 추가 14개 영역 114개 항목으로 구성
ISO 27018	클라우드 서비스 제공자 및 이용자 (IaaS, PaaS, SaaS)	ISO 27002에서 규정한 제어장치에 대한 11가지 구현 지침을 보완한 가이드를 제공 14개 영역 114개 항목으로 구성
CSA STAR	클라우드 서비스 제공자 및 이용자 (IaaS, PaaS, SaaS)	1단계 자가 진단, 2단계 3rdParty에서 STAR인증 성숙도 평가, 3단계 실시간 모니터링 모델 구현의 순서로 진행 IaaS, PaaS, SaaS 사업자별 항목 명시 16개 영역 133개 항목으로 구성

클라우드 침해사고 분석 단계

클라우드 환경의 침해사고 분석

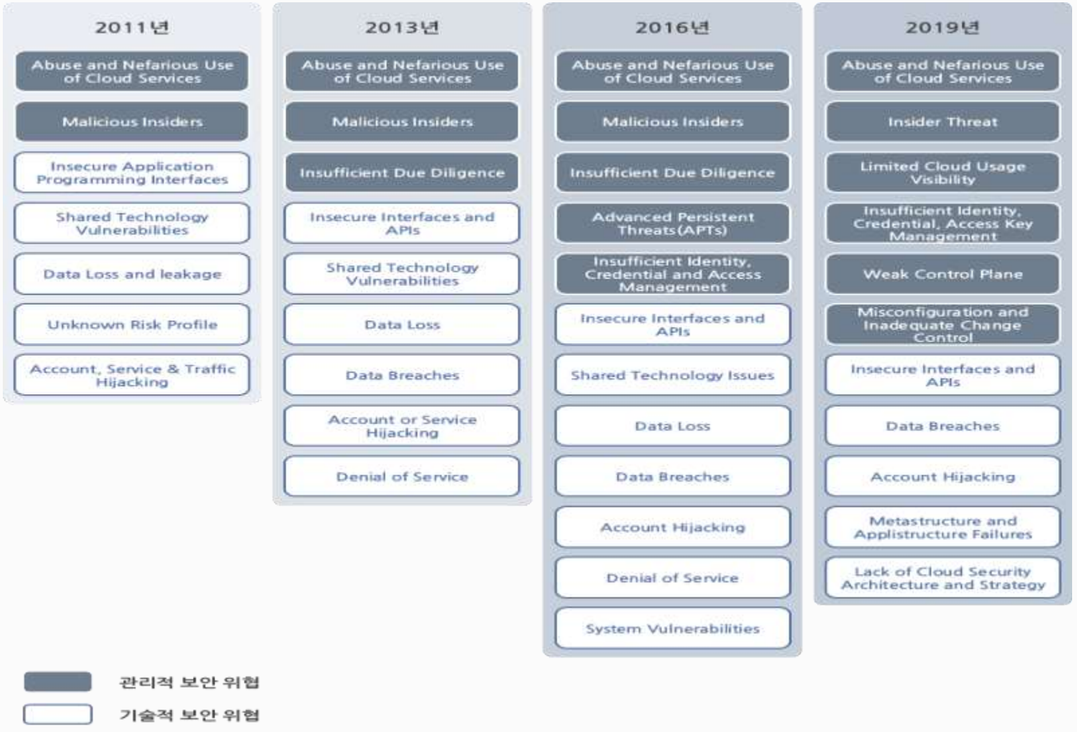
1. 사고 전 준비 단계

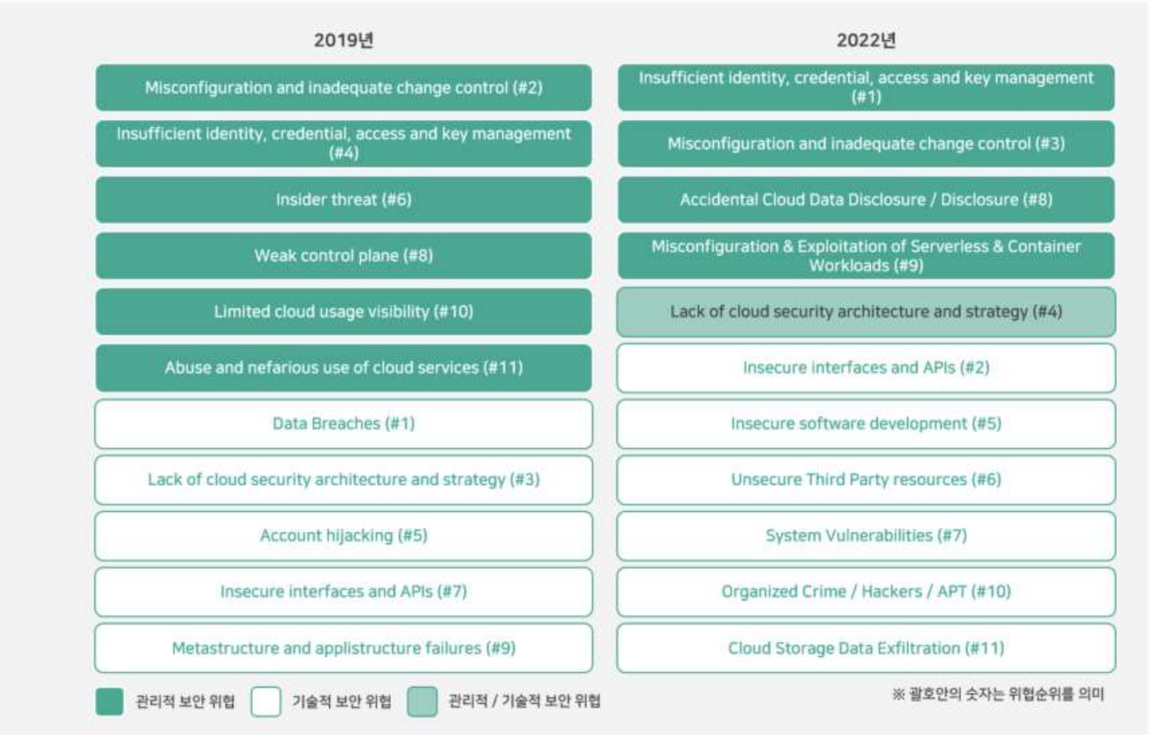
- 보안사고가 발생할 경우 신속하게 대처하기 위해서 침해사고 대응 절차 수립이 필수적
- 일반적으로 침해사고 대응 절차는 사고 전 준비 단계, 사고탐지 및 식별, 증거수집 및 분석, 보고서 작성으로 온프레미스 환경과 클라우드 환경이 동일
- 다만, 클라우드 환경에서는 클라우드 서비스의 어떠한 기술들을 사용하냐에 따라 데이터 수집 및 분석의 가능여부를 확인 가능

구성요소	기술요소
가상화 기술	Resource Pool, Hypervisor(서버 가상화), Partiton Mobility, VLAN, 스토리지
대규모 분산처리	분산 데이터 저장 기술(CODA, Andrew, Apache, Hbase HyperTable 등)
오픈 인터페이스	SOA, Open API, Web Service 등
서비스 프로비저닝	클러스터 관리 기술, 프로비저링 및 스케줄링 등
자원 유틸리티	사용량 측정, 과금, 사용자 계정 관리 등
보안 및 개인정보 관리	플랫폼 보안 기술, 네트워크 보안 기술

클라우드 침해사고 분석 단계

클라우드 환경의 침해사고 분석



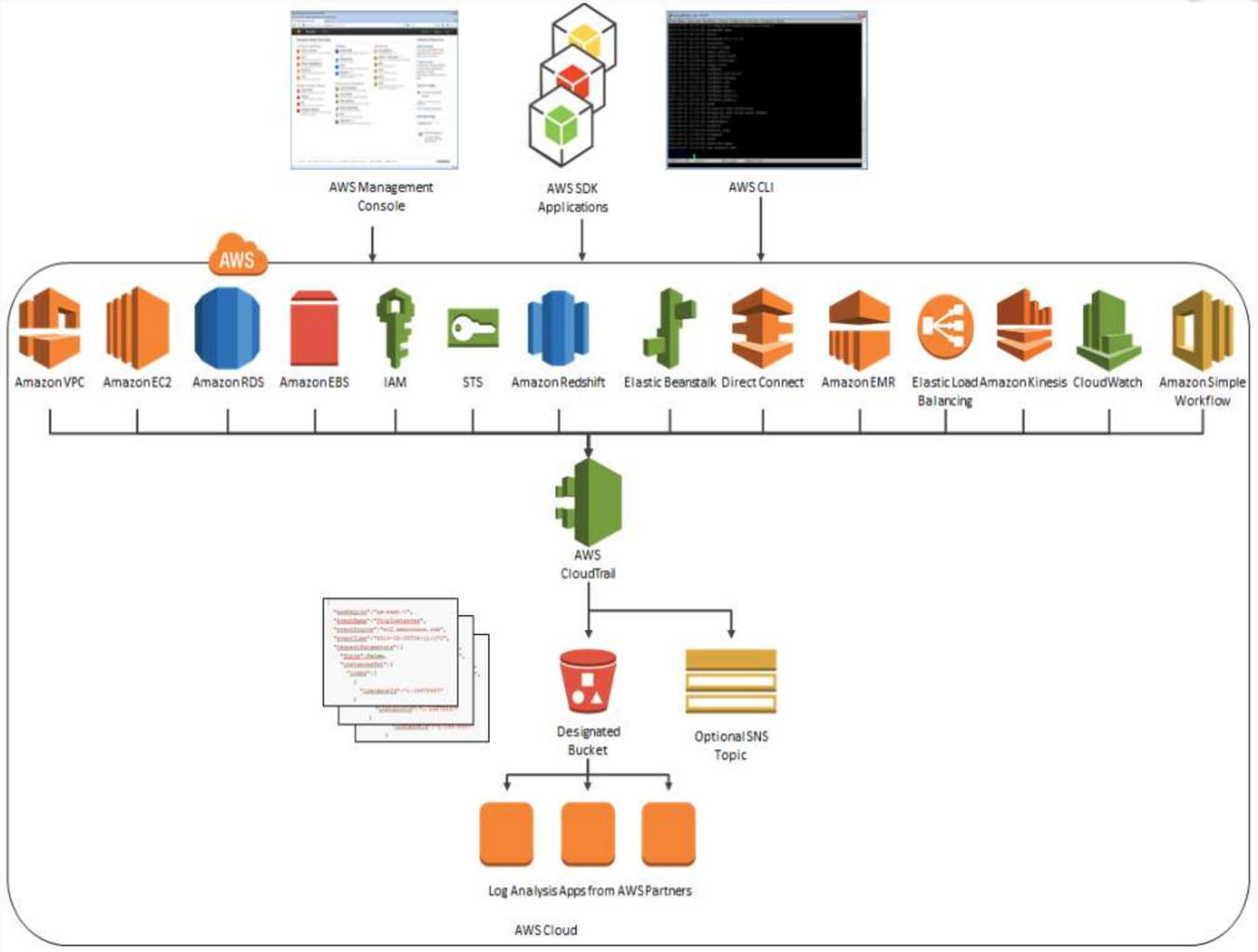


- 클라우드 보안 위협들은 클라우드 컴퓨팅을 사용하는 수많은 이용자들이 대용량의 인프라를 공유하고, 데이터를 중앙집중식으로 관리 및 접근하기 때문에 발생
- 클라우드 서비스 이용이 증가함에 따라 관리적•기술적 보안 위협들의 범위도 점차적으로 ↑

클라우드 침해사고 분석 단계

클라우드 환경의 침해사고 분석

- 보안 위협에 대비하기 위해서는 클라우드 사용자는 보안 설정을 적용하는 것뿐만이 아닌, 주요 시스템의 로깅과 이상 징후 모니터링을 진행
- 클라우드 제공 업체들은 자체적으로 로깅과 모니터링 서비스를 제공(AWS CloudTrail, AWS CloudWatch와 같은 서비스를 주로 사용)
- 주요 시스템의 로깅과 모니터링을 원활하게 하기 위해서는 제공된 서비스의 기본 설정을 사용하는 것이 아닌, 보안 설정을 변경, 비인가된 행위나 침해 시도를 감지



클라우드 침해사고 분석 단계

클라우드 환경의 침해사고 분석

2. 사고탐지 및 식별

- 침해사고 탐지는 시스템 및 네트워크 사용자, 관리자에 의해 탐지되며 침입탐지 시스템, 방화벽과 같은 보안장비에 의해서도 그 세부 기록들을 확인할 수 있으며 클라우드 컴퓨팅 환경도 동일
- 다만 클라우드 컴퓨팅 환경은 중앙집중식으로 관리 및 접근하기 때문에 공격대상이 서버뿐만 아니라 클라우드 서비스를 이용하기 위해 접근하는 계정에 대하여도 확인
- 클라우드 서비스를 제공하는 공급업체들은 보안장비 이외에도 자체적으로 로그들을 기록하는 서비스가 제공
- 많이 사용되는 클라우드 서비스인 AWS에서는 CloudTrail과 CloudWatch 서비스가 제공되는데 해당 서비스에 기록되어 있는 로그들을 활용하여 침해사고 이상징후를 탐지

침해사고 이상증후	Service	AWS CloudTrail EventName(API)
여러 번의 로그인 실패 유휴 상태 및 디폴트 계정의 로그인 시도	Event	ConsoleLogin
관리자가 생성하지 않은 계정 발견	IAM	CreateUser
설명할 수 없는 권한 변경	IAM	DeleteRolePolicy DeleteUserPolicy PutGroupPolicy PutRolePolicy PutUserPolicy
로그 파일·내용의 삭제	CloudTrail	DeleteTrail
	CloudWatch	DeleteLogStream DeleteLogGroup
	EC2	DeleteFlowLogs
서비스 미 제공시간 동안의 시스템 활동	EC2	RunInstances StartInstances

클라우드 침해사고 분석 단계

클라우드 환경의 침해사고 분석

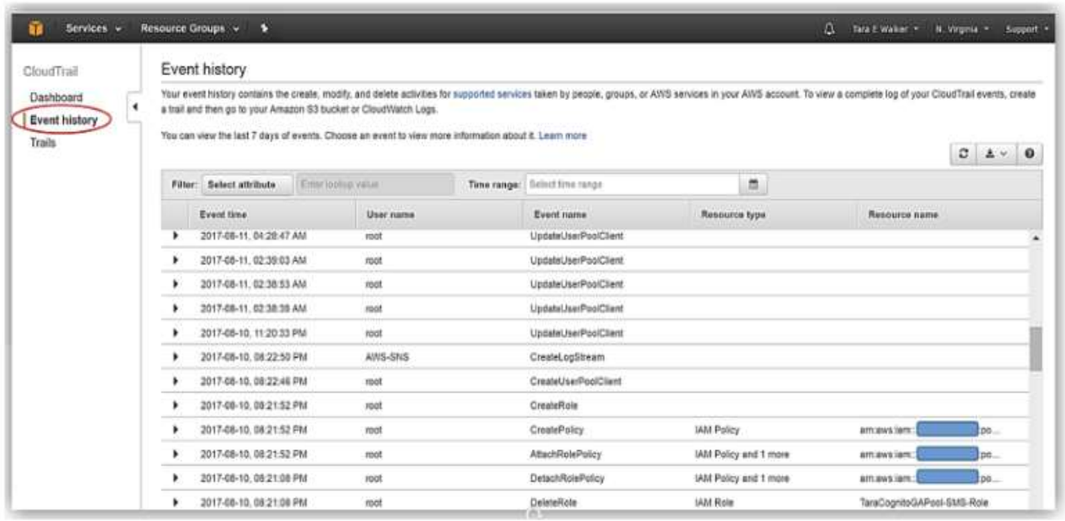
3. 증거수집 및 분석 및 보고서 작성

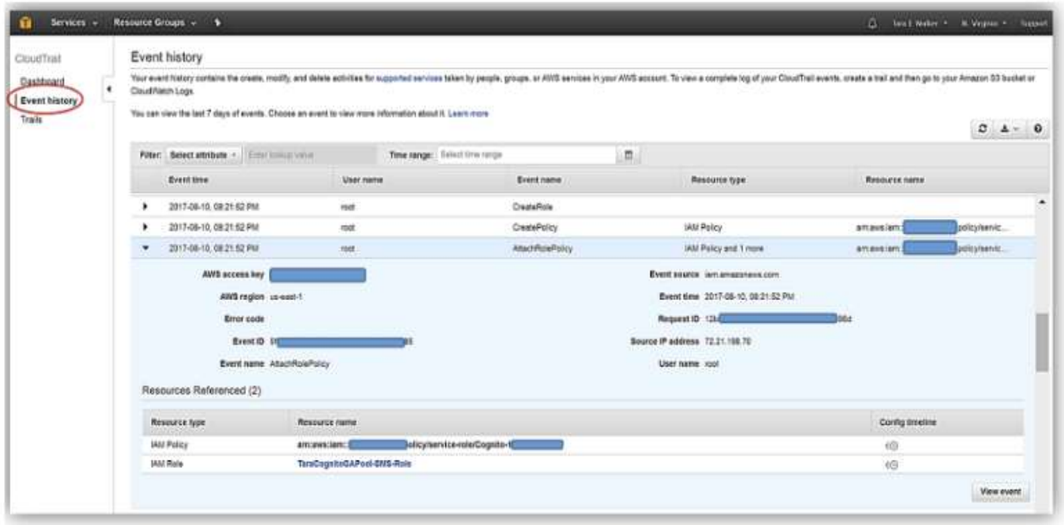
클라우드 환경에서 침해사고 의심 징후가 발견된 경우, 이와 관련된 로그들을 수집하고 가상 환경들을 작동 중지하거나 별도로 보존

클라우드 서비스 로그들과 피해시스템인 가상환경을 보존하지 않고 그대로 작동하게 된다면 피해 규모나 정확한 사고원인을 분석하기 어렵고 2차, 3차 공격경로로 악용되어 사용자가 이용하는 서비스에 문제가 발생할 가능성 ↑

AWS에서 시간, 사용자, 소스IP 주소 등의 정보를 확인할 수 있으며, 지난 90일 동안의 관리 이벤트가 기록이 되기 때문에 90일이 지난 로그는 별도의 백업을 진행하지 않았다면 확인 X

별도의 백업 장비를 구축하지 않았다면 AWS CloudTrail 자체 기능인 내려받기를 통해 이상징후 시점의 로그들을 보관





AWS CloudTrail는 사용자가 이용한 클라우드 서비스 로그를 저장.

클라우드 침해사고 분석 단계

클라우드 환경의 침해사고 분석

별지 제5호 서식

접수번호	FTCCSC-0000

침해사고 분석결과

기 본 정 보			
접수구분	☑FTCCSC ☐NCSC ☐기타	접수일시	0000. 00. 00. 00:00
사 고 정 보			
사고일시	0000년 00월 00일 00:00:00	피해 IP주소	xxx.xxx.xxx.xxx
시스템 용도		운영체제	
사고유형		피해업무	대
공격자IP		공격지역	
사고내용			
분 석 결 과(상세)			
보안대책(재발방지)			

2015년 KISTI 침해사고 대응 분석 보고서
(1/4분기)

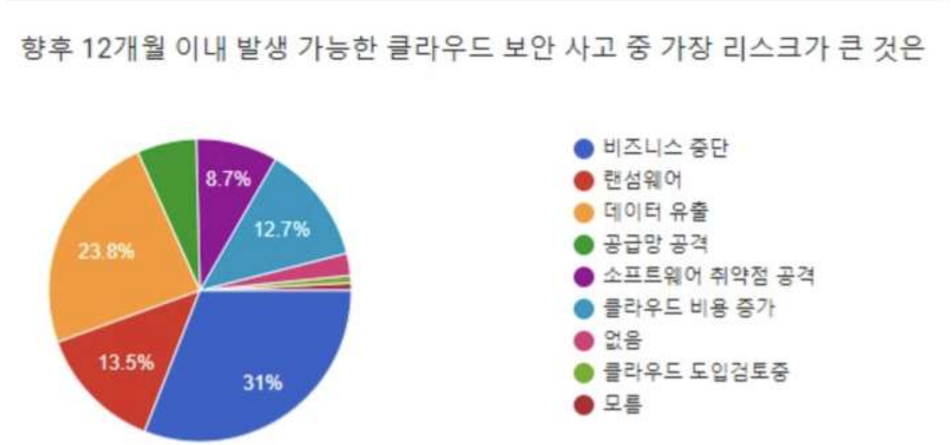
2015. 11.

KiSTi 한국과학기술정보연구원
Korea Institute of Science and Technology Information

- 마지막으로 이상징후가 발견된 시점 전 후를 기점으로 수집•보관된 로그들과 환경 대상으로 분석을 진행한 후 보고서를 작성
- 보고서 작성은 온프레미스 환경의 침해사고 보고서와 동일한 형태로 작성이 되며, 클라우드 컴퓨팅 환경에서만 확인할 수 있는 내용을 확인하여 사실관계 중심으로 작성

결론

클라우드 환경의 침해사고 분석



'제 5회 클라우드 보안 & SECaaS 인사이트 2023' 참가자 대상 설문조사

응답자의 11.9%가 최근 12개월 이내에 한 번 경험했다고 답했으며, 4.8%는 2번 이상 피해를 당했고, 6.3%는 클라우드를 사용하는 동안 여러 차례 피해를 입음.

응답자의 59.5%는 클라우드 보안 사고를 경험하지 않았다고 답했으며, 16.7%는 사고가 발생했는지 여부를 알지 못함(클라우드 보안 사고에 대한 가시성 확보가 시급)

글로벌 트렌드에 비해 클라우드 전환률이 높지 않은 국내 환경에서 1/4 가까운 응답자가 보안사고를 당했다고 답해 보안 대책 마련이 시급

결론

클라우드 환경의 침해사고 분석

기술적 대책	가상 자원에 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 실시 PC, 무선 단말기 등 클라우드 서비스에 접속하는 IT 자원 안전하게 관리 클라우드 시스템 접근에 대한 사용자 인증, 로그인 횟수 제한, 사용자 권한 구분 등 보안설정 적용 시스템 계정 관리는 안전한 패스워드 설정 규칙 적용시켜 주기적으로 변경 개인정보, 기업의 중요 정보는 사전에 암호화하여 저장
관리적 대책	클라우드 컴퓨팅 서비스에 사용된 자산의 변경이 필요한 경우 보안 영향 평가를 통해 변경 운영 중인 클라우드 컴퓨팅 서비스가 네트워크 장애로 중단되지 않도록 지속적으로 모니터링 실시 침해사고 절차 수립 및 발견된 취약점을 관련 조직 및 임직원과 공유하여 처리 클라우드 서비스 도입에 따른 법 규정의 위배사항 발생여부를 파악하고 처리

감사합니다.