RSA Conference 2022 Insight 및 보안 트렌드

SK shieldus

RSA Conference 2022 Insight 및 보안 트렌드

- RSA Conference 2022 행사 개요
- 최신 해킹 Trend 및 주요 사고 사례
- 미국 Privacy 법제 동향 및 공급망 위험관리 소개

SK shieldus

I

RSA Conference 2022 행사 개요

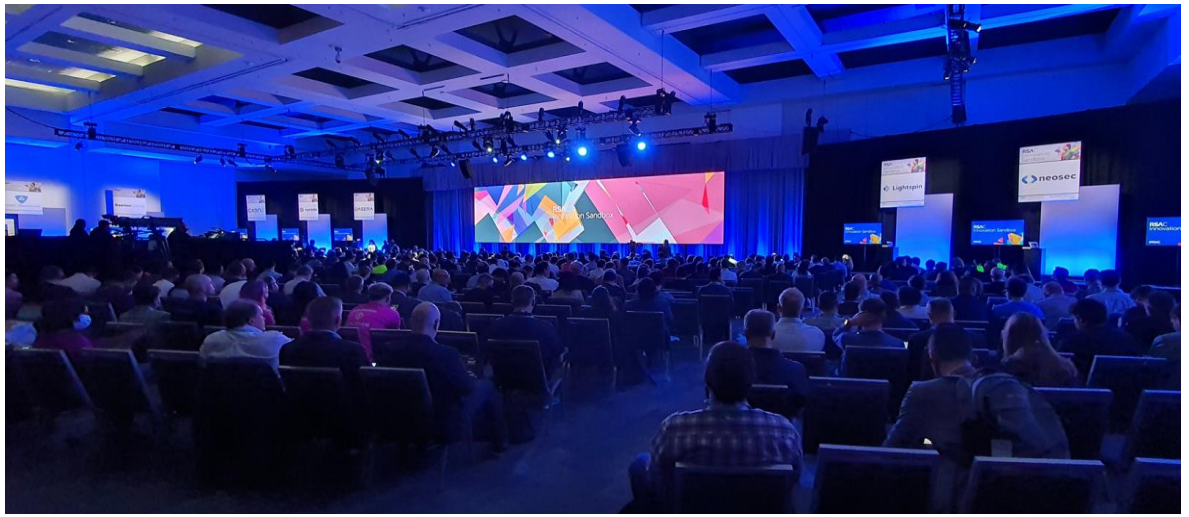
SK shieldus

01 | RSA Conference 2022 개요

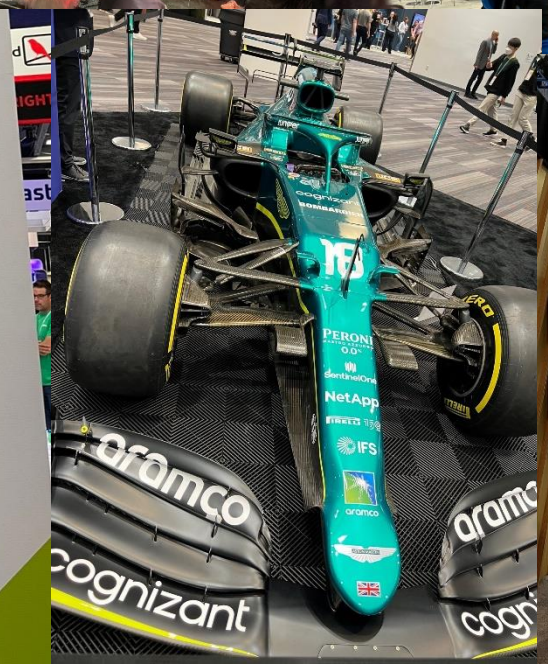
- 기간 : 6월 6일 ~ 9일
- 장소 : Moscone Center, San Francisco & Digital
- 주제 : TRANSFORM
- 주요 내용
  - Innovation Sandbox
  - 25+ Keynotes
  - 350+ Sessions (Cloud, Zero Trust, Privacy, …)
  - 400+ Exhibitors (Early Stage Expo)
  - Vendor Seminar (Qualys Security Conference, Mandiant APJ, IDC Analyst Briefing, …)

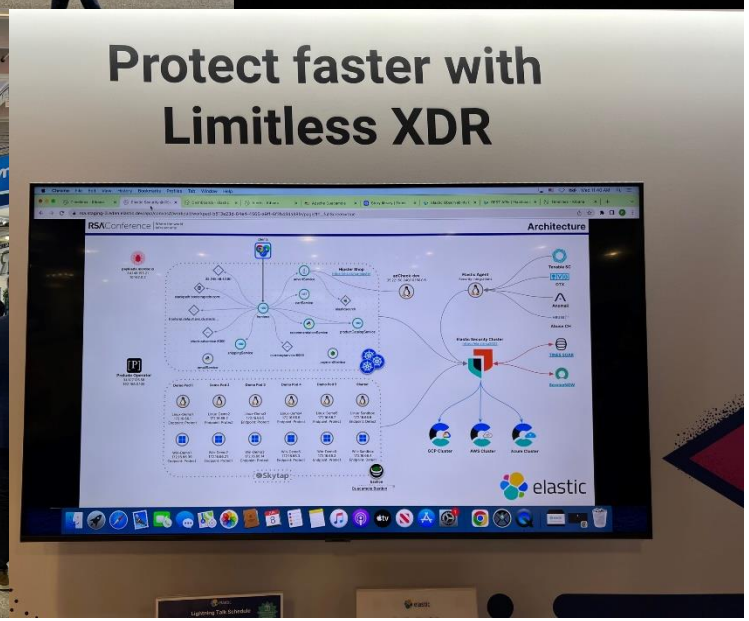
- TRANSFORM (Together, we transform.)
  - 팬데믹 이후의 Cybersecurity 변화 필요
  - RSA Security, RSA Conference 독립운영

02 | RSA Conference 2022 행사 전경



02 | RSA Conference 2022 행사 전경

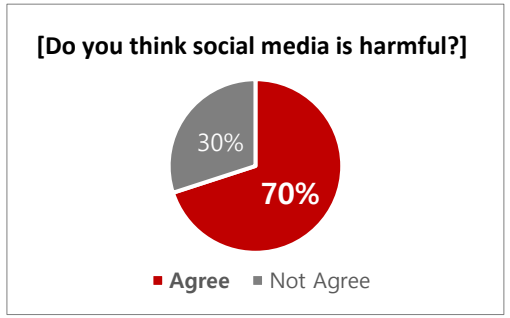




03 | RSA Conference 2022 Keynotes

Soulless to Soulful, Security's Chance to Save Tech (June 07, Trellix)

- **"From soulless to soulful work presents an incredible opportunity for our industry."** (Bryan Palma, CEO, Trellix)
- **Normally at RSA we discuss important topics like AI, anti-ransomware, but, today I only want to talk about PEOPLE.**



- **Social Media 기업의 현재**
  - 과거, Social Media 회사는 세상을 더 가깝게 만들고 Community를 육성한다는 신념으로 인재들을 끌어들임
  - 그러나 그들은 Social Media의 유해성을 방치하고 있으며, **인재들은 신념을 지키지 못하는 회사를 떠나게 됨**
- **'Soulful Work'를 찾는 인재들**
  - 기업을 떠난 인재들은 좀 더 높은 가치를 지향하며 일에 자부심을 가질 수 있는 Soulful Work를 찾고자 함
    ⇨ **사람을 지키는 Cybersecurity가 그들의 지향점과 부합하고 있으며, 이는 Cybersecurity 업계에 놀라운 기회**

- **시간이 갈수록 증가하는 보안 전문가 공급 부족을 해결하고 인재를 끌어들이기 위해서는…**
  - **보안 전문가 집단의 다양성 부족은 수요와 공급 GAP이 주요 원인**
    - 설문조사에 따르면 보안전문가의 78%는 남성, 64%는 백인, 89%는 이성애자. 하지만 Hacker는 국가와 인종, 성별을 넘나드는 다양성 보유
  - **수백만 명의 보안 인재 부족이 남긴 공백을 메우기 위해서는 새로운 접근법 제시 필요**
    - 저 연령부터 Cybersecurity에 대한 조기 인식 개선 필요 (e.g., 장학금/인턴십 프로그램, Community college 프로그램의 확대, 세금감면 등등)
    - 우유산업이 Campaign을 통해 급격히 성장한 것처럼, Cybersecurity도 우리만의 Campaign을 통해 인재문제를 해결할 필요가 있음

- **Introducing "I do soulful work"**
  - **They are doing Soulful Work, just like you do soulful work, and I do soulful work.**

Make the World Better	Give Inspiration	Protect People	Keep the Country Safe

Topics & Tracks for RSAC 2022

- Analytics Intelligence & Response
- Anti-Fraud
- C-Suite View
- Cloud Security & Cloud Sec Ops
- Cryptography
- DevSecOps & Software Integrity
- Hackers & Threats
- Hackers & Threats Advanced
- Human Element
- Identity
- Law
- Machine Learning & Artificial Intelligence
- Open Source Tools
- Partner Perspectives
- Policy & Government
- Privacy
- Professional Development & Personnel Management
- Protecting Data & the Supply Chain
- Risk Management & Governance
- Securing All the Things
- Security Mashup
- Security Strategy & Architecture
- Technology Infrastructure & Operations
- Zero Trust

04 | RSA Conference 2022 Keywords

04 | RSA Conference 2022 Keywords

Ransomware

Supply Chain

Identity

API

Active Directory

Security Operations

Attack Surface

XXDR…

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Identity

Supply Chain

Active Directory

API

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Supply Chain

Identity

API

Active Directory

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Supply Chain

Identity

API

Active Directory

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Identity

Supply Chain

Active Directory

API

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Supply Chain

Identity

API

Active Directory

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Supply Chain

Identity

Active Directory

API

Attack Surface

Security Operations

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Identity

Supply Chain

Active Directory

API

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Supply Chain

Identity

API

Active Directory

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Identity

Supply Chain

Active Directory

API

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

04 | RSA Conference 2022 Keywords

Ransomware

Identity

Supply Chain

Active Directory

API

Security Operations

Attack Surface

XXDR...

Zero Trust

Digital Risk/Reputation

Cloud Native Security Analytics Platform

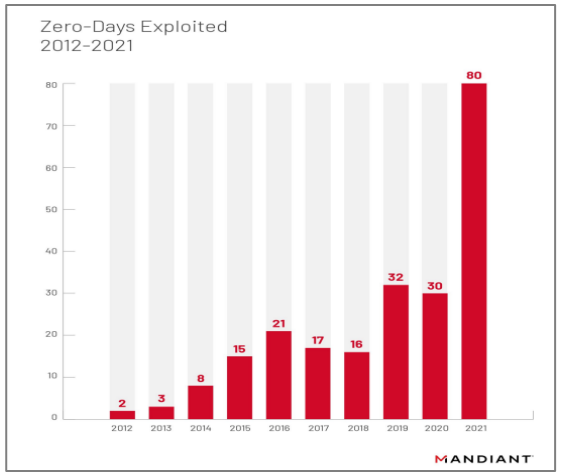
II

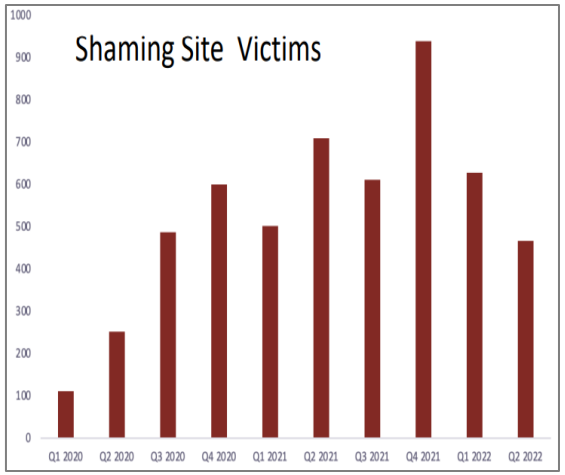
최신 해킹 Trend 및 주요 사고 사례

SK shieldus

01 | RSAC '22년 최신 해킹 Trend

Global Threat Brief: Hacks and Adversaries Unveiled





- **Speaker : Dmitri Alperovitch, Sandra Joyce**
- **주요 내용 : 새로운 공격 그룹 구체적인 사례 및 대응 전략**

○ 국가별 공격 그룹 및 특징

구분	중국	이란	북한
공격그룹	LightBasin / UNC1945	SamSam	-
타깃	통신업체 정부기관	ICS	금융 암호화폐
공격 특징	GPRS Protocol Zero-day	결합공격 (유출, 랜섬)	내부침투 랜섬웨어
대응방안	Non-TCP Protocol 최신 패치 적용	정보유출 탐지	내부자 교육 콜드 스토리지

○ 대응전략

보안 인재 개발 집중 ✚ **효율적 모니터링 강화**

- **내부 침투 해킹 공격 탐지**
  - 시스템 악성코드 탐지
  - 최종 목표전 다단계 탐지
- **사고 대응프로세스 및 훈련**

01 | RSAC '22년 최신 해킹 Trend

The Five Most Dangerous New Attack Techniques

- **Speaker : Ed Skoudis외 4명 / SANS Institute**
- **주요 내용 : 가장 위험한 5가지 공격 기법 기술**

1. **Living Off The Cloud → 동일 Cloud Network Anomaly Traffic 분석**
2. **Multi-factor Authentication → Multi-Factor 변경 절차 강화**
3. **Attacks Against System Backup → 중앙 관리 시스템 액세스 강화**
4. **Mobile Device → Update, 기본 앱 비활성화, Data Backup 등**
5. **Communication Satellites → 원격 접속 이상징후 탐지/차단**

01 | RSAC '22년 최신 해킹 Trend

Hacking Exposed: Next-Generation Tactics Techniques and Procedures

- **Speaker : George Kurtz외 1명 / CrowdStrike**
- **주요 내용 : 차세대 해킹 전술 (기술 및 절차)**
  - **Cloud 환경 Container Server 사용 증가에 따른 공격 증가 예상**
  - **Cloud Container 해킹 시 다른 Container, Host OS 해킹 노출**

    → VM Server와는 다르게 하나의 Host OS 를 공유하기 때문
  - **예상 가능 해킹 시나리오**

    → Host 또는 Container 권한 악용 고객 데이터 접근

    → 다른 Container 데이터 감시, 랜섬웨어 감염
  - **대응방안**

    → 컨테이너화된 시스템 심층 방어 필요

    → 최신패치, 악의적인 런타임 프로세스 모니터링 및 제어

01 | RSAC '22년 최신 해킹 Trend

Ransomware Reality Checklist: 5 Ways to Prevent an Attack

- **Speaker : John Fokker / Trellix**
- **주요 내용 : 랜섬웨어 공격 방지 5가지 방법**
  - **내부 보안 Hole 파악, 대비**
  - **주요 계정 정보 유출 사실을 빠르게 탐지**

    → 정보 유출 모니터링, ZoomInfo/RocketReach 도구 활용
  - **기존 공격자로 부터 공격 패턴 습득**

    → 다른 공격 PlayBook 참고, 솔루션 적용

    → 주로 사용되는 비악성 도구 모니터링 강화
  - **보안 가시성 확보**
  - **침투 단계별 방어 정책 설정**

01 | RSAC '22년 최신 해킹 Trend

Securing Entry Points and Active Directory to Prevent Ransomware Attacks

- **Speaker : Dereck Melber/ Tenable**
- **주요 내용 : 랜섬웨어 공격 진입점 및 AD 보안**
  - **IT 운영자 설문자 중 18%만 AD 보안 위협 관리**
  - **'21년 SolarWinds 공격 백도어 사례**

    → 악성코드 AD 가입여부 확인, 미가입 시 백도어 중단(AD 타깃 전용)
  - **공격자의 전술**

    → 취약한 구성, 관리 권한 계정, 비밀번호 공격

    → 고도화/지속 공격, 백도어 등의 공격 수행
  - **AD 해킹 탐지/대응 전략**

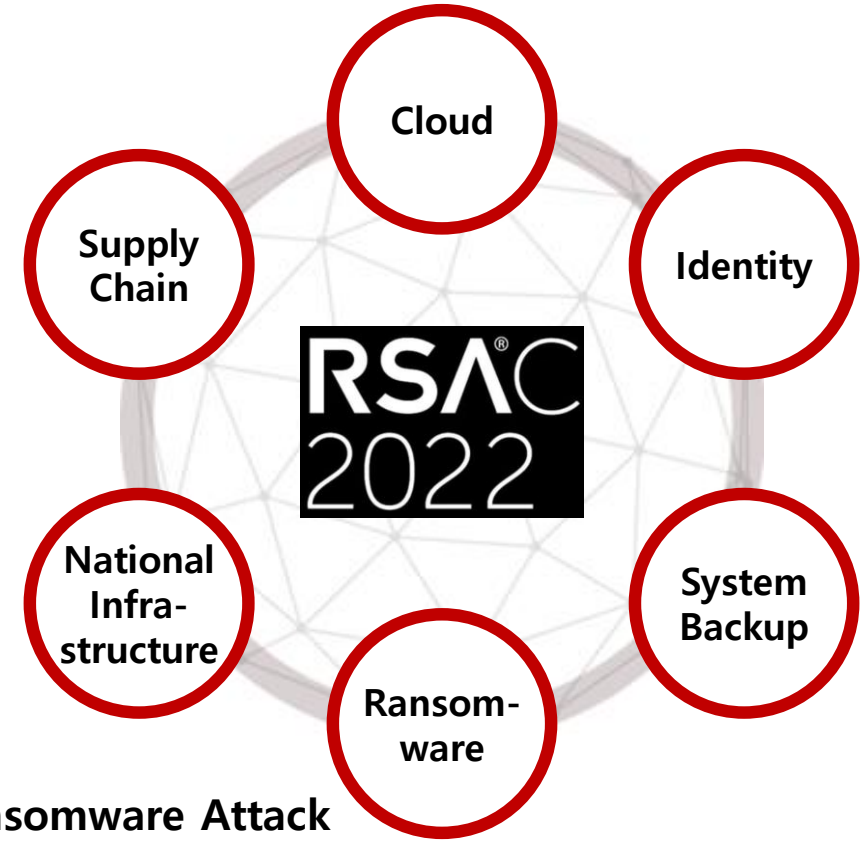
    → 취약 설정 부분 점검, 실시간 자동 탐지/분석

    → 패스워드 관리, 최소 권한, DCSYNC, ZeroLogon 확인

02 | RSAC '22년 최신 6가지 해킹 Trend (요약)

Cloud Target Attack

- Container Server 취약점 악용
- 연동 API 취약점(Code injection, Replace, CSRF, authentication)



Supply Chain Attack

- 공급망 업체 Update Server Target
- 해커 공급망 취약점 연구 지속

Identity Attack

- 유출 계정 입수, 추가 공격 수행
- Fail open 접근 방식 남용 MFA 우회 기법

National Infrastructure Attack

- 러시아-우크라이나 전쟁 통신위성 해킹
- 국가간 분쟁 및 기반 시설 Target

System Backup Attack

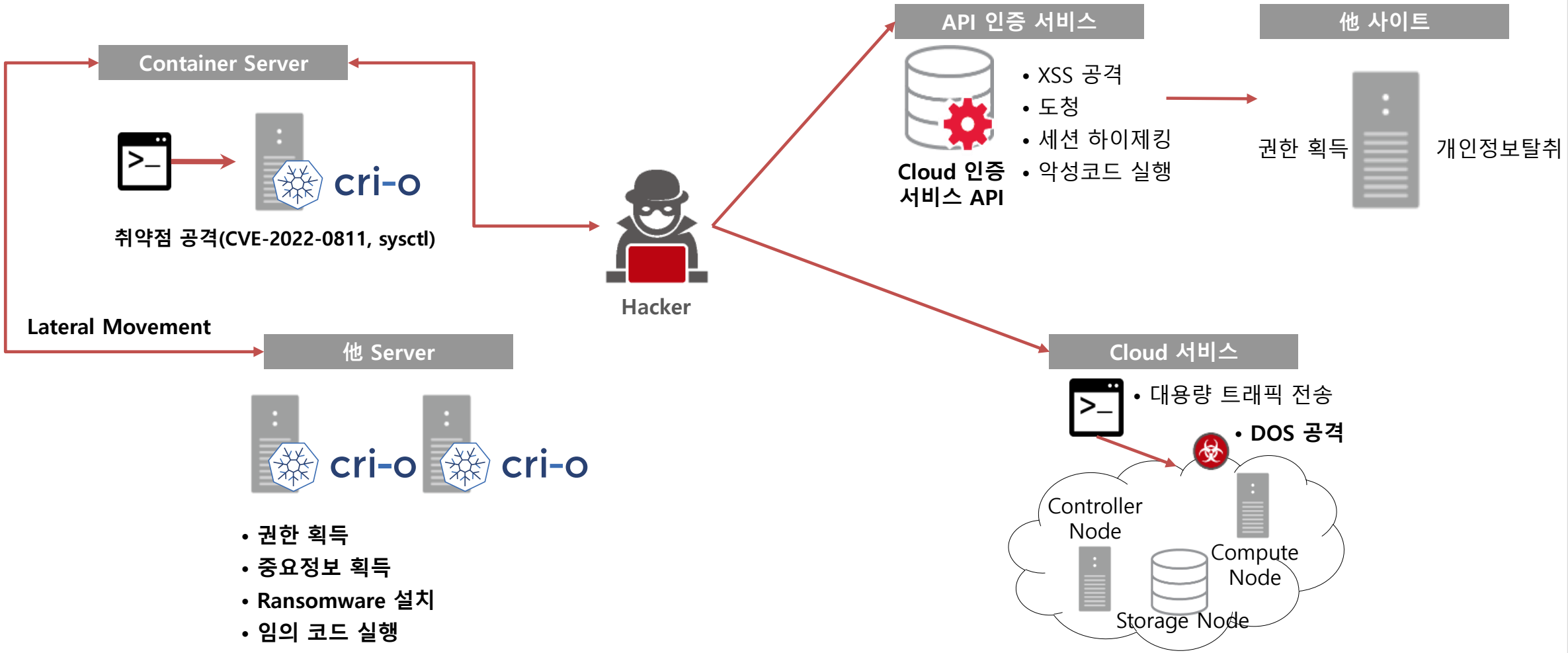
- 벤더 백업 시스템 취약점 다수 존재
- IBM, Veritas, Kaseya, Dell 등

Ransomware Attack

- 금전 획득이 용이한 랜섬웨어 공격 확대
- 한층 악랄해진 협박 방법 진화

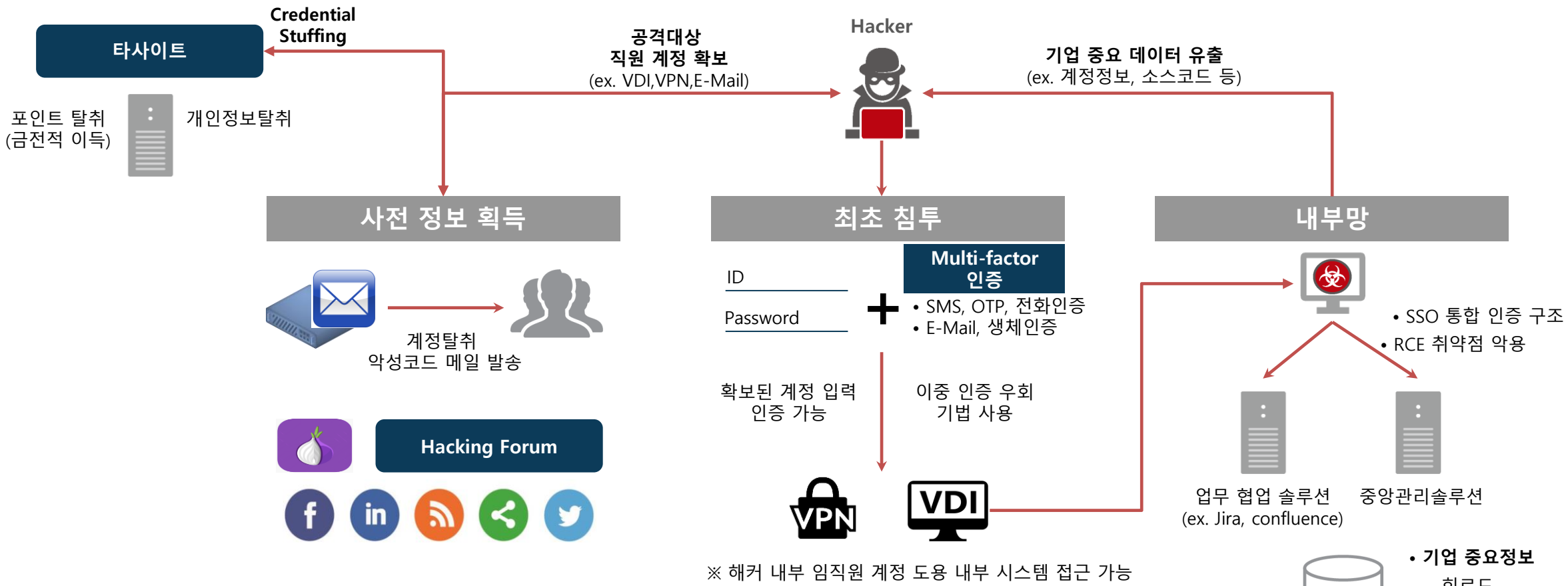
03 | '22년 주요 보안사고 사례

Cloud Attack



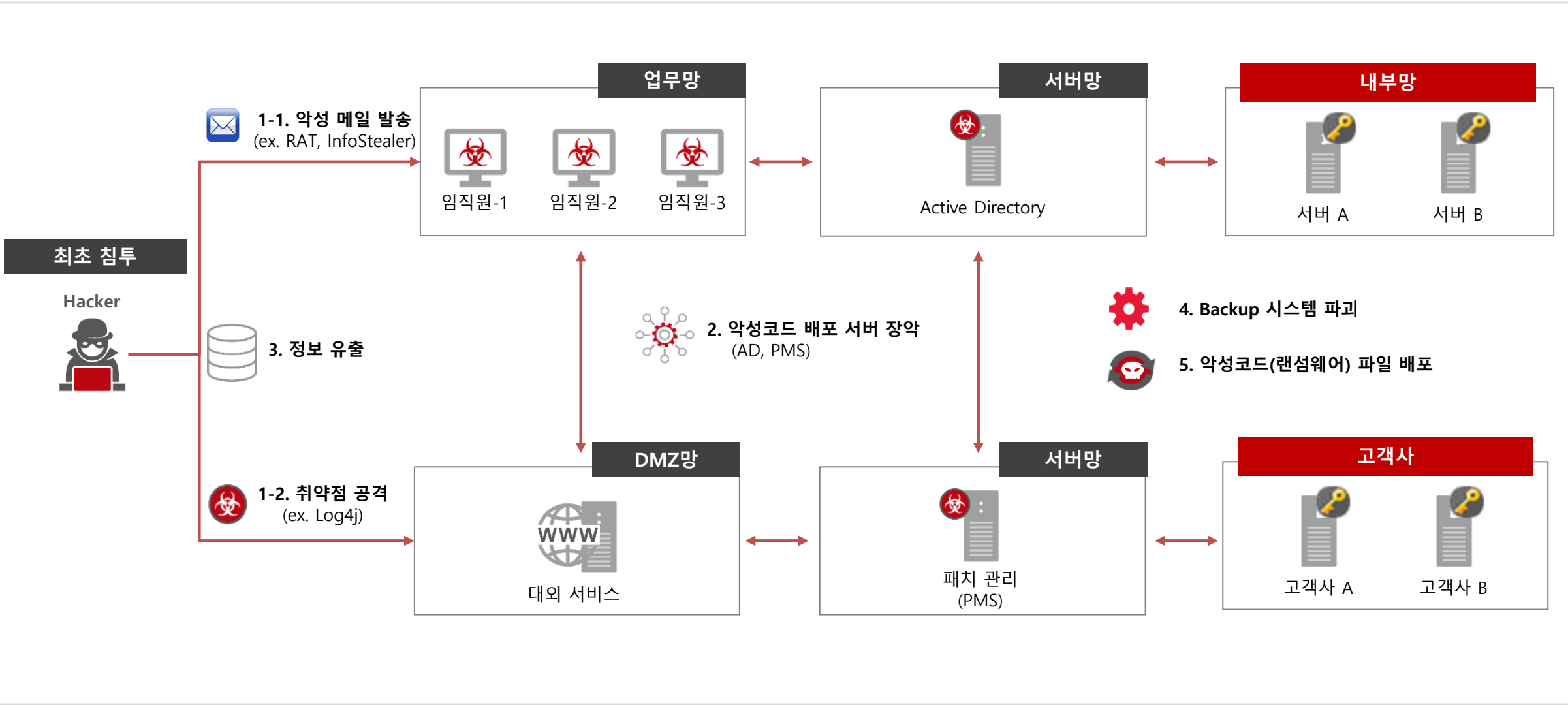
03 | '22년 주요 보안사고 사례

Identity Attack



03 | '22년 주요 보안사고 사례

Supply Chain + Ransomware Attack

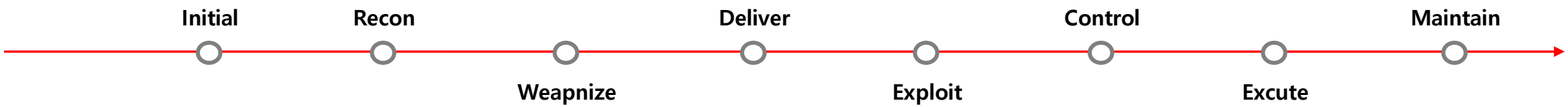


04 | '22년 주요 보안사고 사례 원인 및 대응방안

【사고 유형】	【사고 주요 원인】	【대응 방안】	【솔루션/서비스】
1 "Cloud Taget Attack"	• Container Server 취약점 - 보안 업데이트 미흡, RCE 취약점 존재 - 불필요한 계정 악용, 패키징 파일 악성코드 • 연동 API 취약점 - Code injection, Replace, CSRF authentication등 민감한 데이터 노출	• **Cloud Container Environment 강화** - 최신 업데이트 유지, 정기 로그 점검 - 사용자별 권한 강화, 이미지 취약점 검사 • **API 취약점 점검 강화** - 평문노출, Key 유출, 명령 조작 등 - 사용 권한통제, 이상행위 탐지	✓ Container 보안 솔루션 ✓ API 보안 솔루션
2 "Identity Attack"	• 임직원 계정 유출 모니터링 미흡 • Multi-factor 인증 미흡 • 원격 담말 접근 보안 정책 미흡 • 임직원 이상 행위 모니터링 미흡 • 업무협업, 중앙관리 시스템 취약점 존재 • 악성코드 탐지, 중요자료 암호화 미흡 • 정보 유출 모니터링 미흡	• **임직원 계정 유출 모니터링 강화** • **Mult-Factor 예외구간 점검(소유기반 적용)** • **사전 승인•지정 단말 접근 정책 적용** • **임직원 이상 행위 모니터링 체계** • **업무 협업, 관리 시스템 보안 패치** • **중요자료 식별 및 암호화** • **정보 유출 탐지/차단 체계 구축**	✓ 계정 유출 탐지 솔루션 ✓ E-Mail APT ✓ Multi-factor 인증 솔루션 ✓ FDS(Fraud Detect System) ✓ 패치•취약점 관리 시스템 ✓ N/W APT, EDR 솔루션 ✓ 암호화 솔루션 ✓ SIEM 솔루션
3 "Supply Chain + Ransomware Attack"	• E-Mail 악성코드, 웹 취약점 탐지 미흡 • PC, 서버 악성코드 미탐지 • PMS 배포 전 파일 점검 및 모니터링 미흡 • 백업 시스템 RCE/LPE 취약점 존재 • 랜섬웨어 탐지 미흡	• **예외처리 도메인 등록** • **PC, 서버 악성코드 탐지 체계 강화** • **PMS 배포 점검 체계 및 로그 분석 강화** • **백업 시스템 패치 최신화** • **정보 유출 탐지/차단 체계 구축**	✓ E-Mail APT ✓ N/W APT, EDR 솔루션 ✓ SIEM 솔루션

05 | 22년 주요 보안사고 대응 (결론)

MITRE ATT&CK* Framework (*Adversarial Tactics, Techniques, and Common Knowledge)



대응 방안

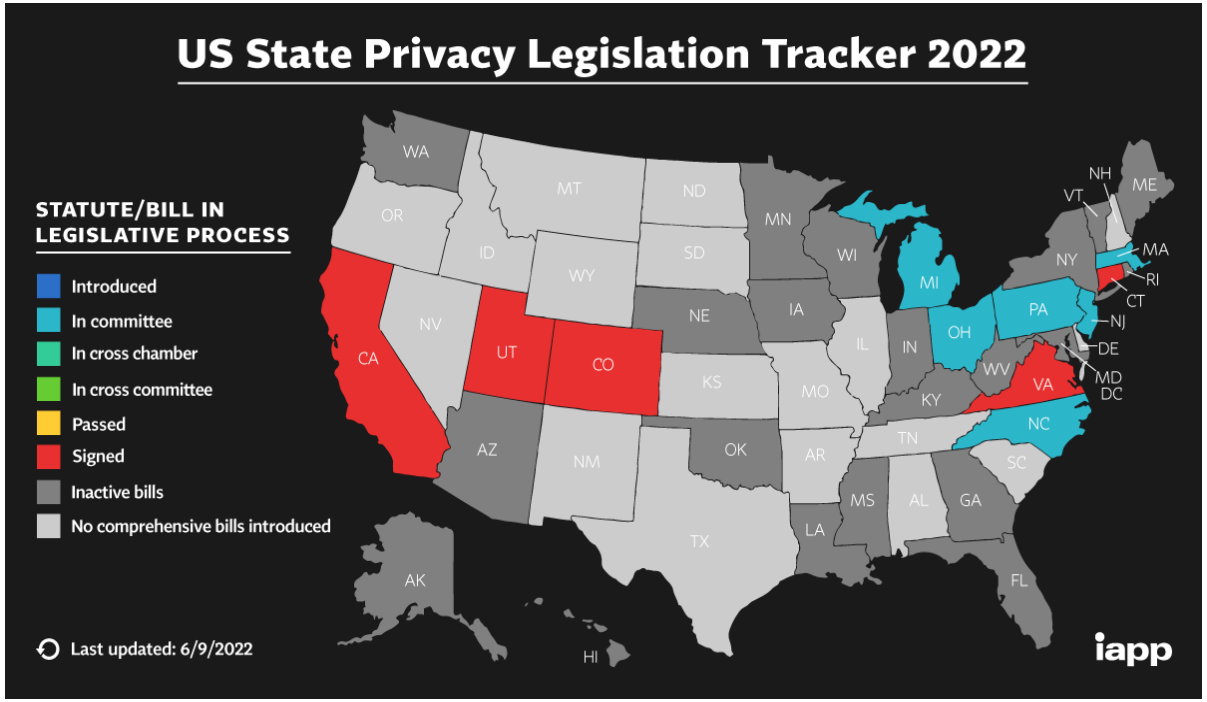
Security 영역	Web Security Cloud Security IoT Mobile Security Application Security N/W & Infrastructure Security Security Consulting Identity & Access Management Blockchain	Endpoint Security MSSP	Security Ops & Incident Response Digital Risk Management	Data Security	Messaging Security Floud & Transaction Security		Threat Intelligence Risk & Compliance
Human	Security strategist (CISO, CPO)	Operation	developer	Security Expert	Security Expert (Mornitoring, analyst)		
Facility & Process	SOC	보안 이벤트 탐지/분석 체계	보안교육 (담당자, 임직원)	주기적 진단 (침해사고흔적, 취약점)	최신 패치 정보 수집/적용		보안 인증 (ISMS, ISO27001 등)

III

미국 Privacy 법제 동향 및 공급망 위험관리 소개

SK shieldus

01 | 미국 Privacy 법제 동향



- Privacy Act 시행
  - 5개주●: 캘리포니아, 콜로라도, 코네티컷, 버지니아, 유타
  - CCPA → CPRA(23년 1월 시행예정)
    * CCPA: California Consumer Privacy Act
    * CPRA: California Privacy Rights Act
- Privacy Act 의회 발의
  - 7개주●: 메사추세츠, 미시건, 뉴저지, 뉴욕, 오하이오, 노스캐롤라이나, 펜실베니아
- 그 외 여러 주에서 개인정보보호법 입법을 위한 많은 시도가 있어 왔음●

- 최근 연방차원의 개인정보보호법 도입을 위한 논의가 진행 중이며, 몇몇 법안이 발의되어 심의 중에 있음

주요 법안 내역	
H.R.1816 -	Information Transparency & Personal Data Control Act
S.1494 -	Consumer Data Privacy and Security Act of 2021
S.2134 -	Data Protection Act of 2021
S.2499 -	Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act(SAFE DATA Act)

02 | 미국 Privacy 법제 동향_CCPA → CPRA

CPRA는 '23년 1월 1일 시행예정

- 소비자의 권리와 기업의 의무 강화
- 미국 최초의 개인정보보호 전담 집행기관 설립 근거 마련

CPRA 주요 내용

주요 변경 사항	
적용대상 축소	소규모 사업체 중 연간 5만~10만 명의 개인정보를 관리·처리하는 사업체를 CPRA 적용대상에서 제외
민감정보 정의 규정	민감정보 개념을 새롭게 도입하고 민감정보의 이용 및 공개를 제한
소비자 권리 강화	소비자에게 ①부정확한 정보에 대한 정정요구권 ②자동화된 의사결정 거부권 ③민감정보 공유 및 사용 거부권 등을 추가적으로 부여
기업의 의무 강화	사업체에게 ①개인정보보호 의무 등을 명시한 계약 작성 의무화 ②기업의 보안 절차 등을 합리적으로 구현하여 개인정보를 보호하는 보안책임을 부담하는 등 기업 의무 강화
개인정보 감독기구 설립	캘리포니아 개인정보 감독기구(CalPPA: California Privacy Protection Agency) 창설을 위한 근거조항이 신설되어, 개인정보보호법 위반에 대한 행정벌금을 부과할 근거를 마련함

시사점

- Privacy 관련 주법 뿐 아니라 연방 법률의 제/개정에 대한 모니터링으로 Business에 미칠 영향에 선제적으로 대응해야 하며,
- Global 기업은 개인정보보호 체계를 국내 Compliance 대응 만이 아니라, 미국/EU/중국 등 다양한 국가에 대응할 수 있는 체계를 수립하여 유지해야 함

* 민감정보: 사회보장번호, 운전면허증, 신분증이나 여권번호, 금융계좌정보, 신용카드 정보, 암호, 접속 자격 증명 등

03 | 공급망 위험관리(SCRM)

A SUPPLY CHAIN IS ONLY AS STRONG AS ITS WEAKEST LINK

효과적인 SCRM 구축을 위한 프로세스 가이드 by CISA

1 IDENTIFY	2 MANAGE	3 ASSESS	4 KNOW	5 VERIFY	6 EVALUATE
WHAT? The People	WHAT? The Security and Compliance	WHAT? The Components	WHAT? The Supply Chain and Suppliers	WHAT? The Assurance of 3rd Parties	WHAT? The Review
SCRM 실행을 위한 조직 구성	공급망 보안정책 및 지침 제정	공급받은 HW, SW, 서비스 목록 파악	공급망의 구조 파악	공급자의 보안현황 평가방침 결정	SCRM 요구사항 점검 및 모니터링

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

- 국가의 주요 기반시설에 대한 물리적, 사이버 위협으로부터 보호하는 임무 수행
- 2018년 ICT SCRM TF 발족 → 민관 협력으로 ICT 공급망의 보안강화 방안 개발 연구 수행

[Backup] System Backup 취약점 List

Product	CVE	Explanation
Veeam	CVE-2022-26500	REC as Local System
IBM Container Backup	CVE-2022-24921	DoS
Veritas Backup Exec	CVE-2021-27877	Execute command on agent
Kaseya Unitrends Backup	CVE-2021-43044	(multiple vulnerabilities)
Dell EMC Cloud Disaster REC.	CVE-2021-44228	Log4j
NetApp	CVE-2022-24921	DoS (Golang issue)

[Backup] 주로 사용되는 비악성 도구 List

◘ Non-Malicious Tools by Cyber Criminals

Native OS Binaries	Percentage	MITRE Technique
Windows Command Shell (CMD)	53.44%	T1059.003
PowerShell	43.92%	T1059.001
WMI/WMIC	33.86%	T1218 T1564.004
Rundll32	24.34%	T1218.011 T1564.004
Regsvr32	14.29%	T1218.010
Schtasks	12.70%	T1053.005
MSHTA	10.05%	T1218.005
Excel	8.99%	T1105
Net.exe	7.94%	T1087 & Sub-techniques
Certutil	4.23%	T1105, 1564.004 T1027
Reg.exe	3.70%	1003.002 1564.004

Administrative Tools	Percentage	MITRE Technique	Info
Remote Services	35.98%	T1021.001	AnyDesk
		T1021.004 T1021.005	ConnectWise Control
			RDP
			UltraVNC
			PuTTY
			WinSCP
Archive Utilities	6.35%	T1560.001	7-Zip
			WinRAR
			WinZip
BITSAdmin	3.70%	T1105 T1218 T1564.004	
ADFind	2.65%	T1016 T1018 T1069 & Sub-Techniques, T1087 & Sub-techniques T1482	
PsExec	2.12%	T1569.002	
Fodhelper.exe	0.05%	T1548.002	

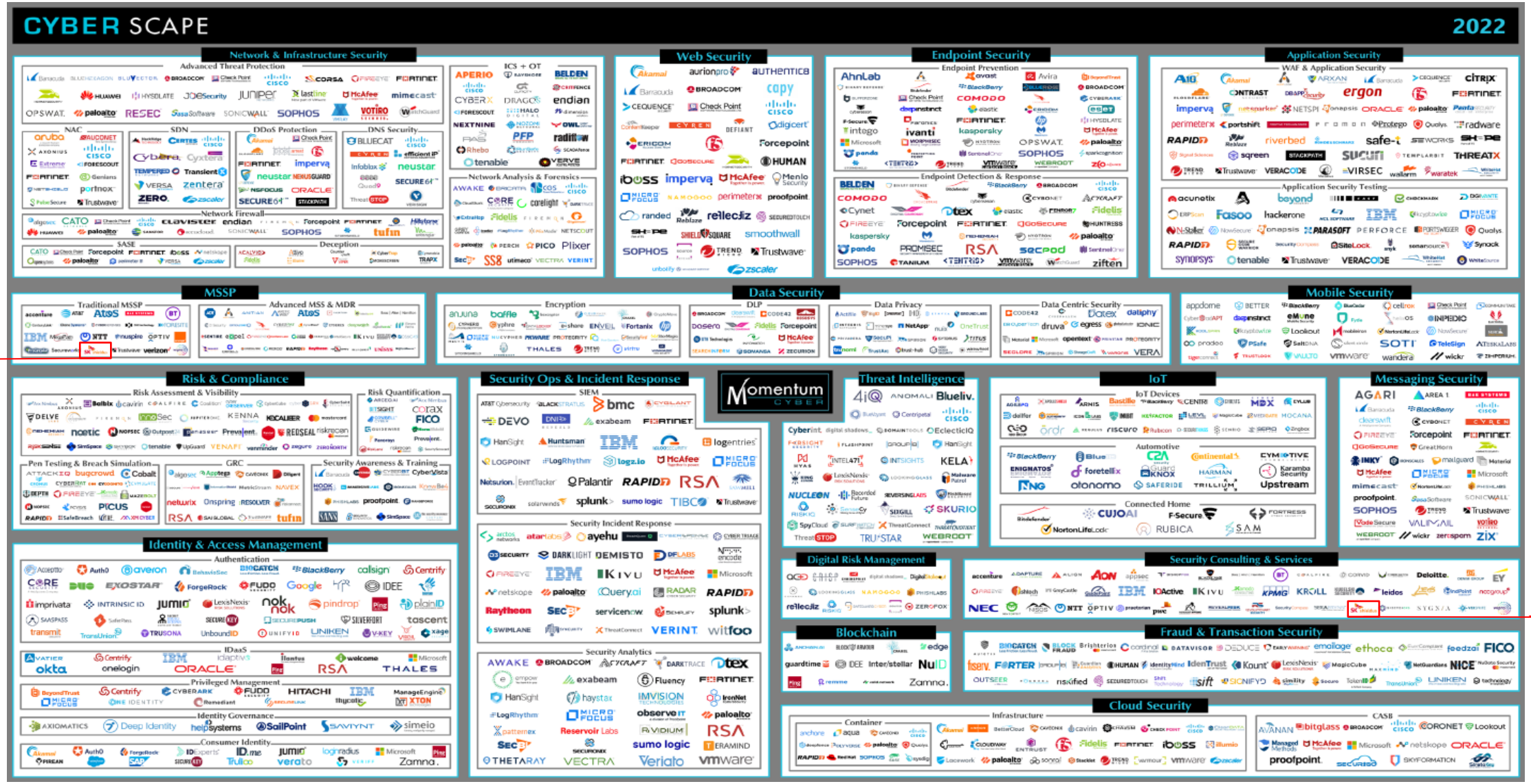
[Backup] 자주 사용되는 CVE Code List

□ Non-Malicious Tools by Cyber Criminals

- All major groups were quick to leverage CVEs over the last 2 years
- Initial Access, RCE or LPE
- Most observed: MS Exchange, SolarWinds Serv-U, Log4J, Accellion, SonicWall, PrintNightmare and SMBv1

CVE-2021-34523	CVE-2021-26084
CVE-2021-34473	CVE-2010-2861
CVE-2021-31207	CVE-2021-36942
CVE-2021-26855	CVE-2021-34523
CVE-2021-4044	CVE-2021-34527
CVE-2021-35211	CVE-2021-1675
CVE-2021-27104	CVE-2021-28799
CVE-2021-27103	CVE-2021-20016
CVE-2021-27102	CVE-2021-27065
CVE-2021-27101	CVE-2021-27065
CVE-2021-44228	CVE-2021-26858
CVE-2021-31206	CVE-2021-26857
CVE-2021-45105	CVE-2020-5135
CVE-2021-45046	CVE-2020-1472
CVE-2021-44832	CVE-2018-13379
CVE-2021-4104	CVE-2018-13374
CVE-2021-21972	CVE-2017-0148
CVE-2021-34473	CVE-2017-0147
CVE-2020-12812	CVE-2017-0146
CVE-2019-5591	CVE-2017-0145
CVE-2018-13379	CVE-2017-0144
CVE-2021-36942	CVE-2017-0143

[Backup] CYBER SCAPE



감사합니다!

SK shieldus