통합 보안 플랫폼 기업, 지니언스

Cybersecurity Trends for 2025

Jul 2025
CTO/미국법인장
김계연

Genians

김계연

한글과 컴퓨터

- 첫 직장 (1994), 아래한글 - PC통신
- 인터넷 사업부 - 두산정보통신 매각
- 첫 해외출장 COMDEX 1995 (Atlanta, USA)

Yahoo! Korea

- 창립멤버 (1996), Chief Engineer
- Setup, Localization (한글화, 한글검색엔진)

어울림정보기술

- 창립멤버 (1997), 연구소장
- KOSDAQ 상장 (2002년)
- 국내 방화벽(Firewall), 가상사설망(VPN) 1위
- 글로벌 3개국 (미국, 일본, 태국) 진출 (1999 - 2004)

지니언스

- 2005년 설립, 공동설립자
- KOSDAQ 상장 (2017년)
- 국내 NAC/EDR 시장점유율 1위 (70%+)
- 2016년 미국법인 설립
- 미국(CA,TX), UAE(두바이), 인도(뱅가루루), 한국(안양)

LinkedIn

01.

EO 14028
Improving the Nation's Cybersecurity

미국 정보보호 시장 동향

사건의 시작

- SolarWinds (2020), MS Exchange (2021) 취약점으로 상당수의 연방 정부기관 침해

행정명령 14028

Improving the Nation's Cybersecurity
May, 2021

- 1장: 정책 (사이버 사고 예방/탐지/평가를 최우선 과제, 민간협력 강조)
- 2장: 위협 정보공유 장벽제거 (정부와 민간의 정보공유 확대)
- 3장: 사이버보안 현대화 (Zero Trust)
- 4장: 공급망 보안 (SSDF, SBOM)
- 5장: 사이버 안전 심의 위원회 설치 (중대 보안사고에 대한 민관 조사 협력)
- 6장: 보안 취약점 및 사고대응 Playbook 표준화
- 7장: 취약점 및 사고 탐지 개선 (EDR 배포계획 수립)
- 8장: 연방정부 사고조사 및 대응 능력 강화

사이버보안 현대화

연방 정부는 보안 모범 사례를 채택하고, **제로 트러스트 아키텍처로** 나아가며, SaaS, IaaS, PaaS를 포함한 **안전한 클라우드 서비스로의 이동을 가속화**해야 합니다. 또한, 사이버 보안 위험을 식별하고 관리하기 위한 분석을 추진하는 **사이버 보안 데이터에 대한 접근을 중앙화**하고 간소화하며, 이러한 현대화 목표에 부합하는 기술과 인력에 투자해야 합니다.

- Cloud First (2011), Cloud Smart (2018)
  - Kubernetes 및 Cloud Native로 인한 IT 시스템 현대화 성숙단계
  - Network Policy, Service Mesh와 같은 보안 PEP가 내재화
  - Cloud 전문 보안솔루션 CSPM, CWPP, CNAPP, CIEM…
  - FedRAMP 인증제도 확산
- End to End 보안
  - Privacy를 위해 종단간 보안이 점점 강화됨 (애플, 구글, 만리방화벽 한목)
  - 완전한 종단간 암호화 추구 (HSTS, Public Key Pinning, QUIC)
  - Man-in-the-Middle 방식의 경계망 보안제품이 무용지물

미국 정보보호 시장 동향

제로 트러스트

- Just-in-Time, Just-Enough, Always Verify
- M-22-09: ZT 5개의 기둥에 대한 구체적인 Action들을 명시 (Jan, 2022)
- 개별 솔루션을 이어주는 개방형 표준 기반 PDP (Policy Decision Point)
  - SAML2: 인증(사람/기기)의 중심, OPA: 보안을 App에 통합
- 그 복잡성으로 인해 관리형 보안 서비스 시장 확대 (MSSP)
  - vSOC 서비스, SASE/SSE를 통한 All-in-One 보안 서비스

공급망 보안

M-22-18

- Secure Software Development Framework (SSDF)
  - NIST SSDF v1.1 (Feb, 2022), CISA Self-Attestation Form (Mar, 2024)
  - 2024년 9월부터 연방정부에 납품되는 모든 소프트웨어 필수
- Software Bill of Material (SBOM)
  - NTIA Minimum Elements for SBOM (Jul, 2021)
  - SBOM 공개 논란: 공격자의 악용 (RSAC 2024 Session)
- Open Source 보안
  - 소프트웨어에 탑재된 OSS가 변조되지 않았음을 보증
  - Sigstore, SLSA (변조불가한 호스팅 환경에서 스크립트만으로 빌드)
  - XZ 라이브러리 사건으로 새로운 국면 (Micro Service Architecture 필요성)

취약점 및 사고 탐지 개선

- M-21-31: 감사기록 수준 및 공유에 대한 규정
- M-22-01: 연방정부 기관에 대한 EDR 배포계획 수립
  - 정부 전체의 가시성을 위해 CISA에서 중앙 집중식 관리
  - 2024년 4월 현재 60개의 기관에 EDR 구축 완료 (청문보고1, 청문보고2)

02.

Understanding US Cybersecurity Market

미국 정보보호 시장 동향

Market Cap (Jul 15, 2025)

Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	Palo Alto Networks PANW	$128.19 B	$192.25	0.80%		USA
2	CrowdStrike CRWD	$117.96 B	$473.28	0.61%		USA
3	Fortinet FTNT	$80.31 B	$104.93	1.90%		USA
4	Cloudflare NET	$64.80 B	$186.97	2.23%		USA
5	Zscaler ZS	$44.98 B	$288.90	0.77%		USA
6	Check Point Software CHKP	$23.70 B	$218.78	0.86%		Israel
7	Leidos LDOS	$20.62 B	$160.21	2.11%		USA
8	CyberArk Software CYBR	$18.85 B	$374.81	0.59%		Israel
9	Gen Digital GEN	$18.55 B	$29.91	0.37%		USA
↑1 10	Rubrik RBRK	$16.89 B	$87.34	1.75%		USA
↓1 11	F5 FFIV	$16.69 B	$290.76	1.15%		USA
12	Okta OKTA	$15.94 B	$91.10	0.95%		USA
13	SailPoint SAIL	$11.33 B	$20.36	1.31%		USA
14	Akamai AKAM	$10.93 B	$76.80	0.79%		USA
15	360 Security Technology 601360.SS	$10.00 B	$1.43	1.69%		China
16	Trend Micro 4704.T	$8.32 B	$63.39	0.25%		Japan
17	Commvault CVLT	$7.42 B	$166.73	1.68%		USA

미국 정보보호 시장 동향

FedRAMP Marketplace

Provider ↕	Service Offering ↕	Service Model ↕	Impact Level ↕	Status ↕	Authorizations ↕	Reuse ▼
okta	Okta IDaaS Regulated Cloud	SaaS	Moderate	FedRAMP Authorized	23	332
Google	Google Workspace	SaaS	High	FedRAMP Authorized	14	312
Microsoft	Office 365 Multi-Tenant & Supporting Services	SaaS	Moderate	FedRAMP Authorized	88	233
Qualys.	Qualys Cloud Platform	SaaS	Moderate	FedRAMP Authorized	10	200
slack	Slack	SaaS	Moderate	FedRAMP Authorized	11	181
servicenow	Government Community Cloud	PaaS SaaS	High	FedRAMP Authorized	76	173
DUO	Duo Federal	SaaS	Moderate	FedRAMP Authorized	11	131
CROWDSTRIKE	Falcon Platform	SaaS	Moderate	FedRAMP Authorized	20	124
DATADOG	Datadog	SaaS	LI-SaaS	FedRAMP Authorized	1	104
GitHub	GitHub Enterprise Cloud	SaaS	LI-SaaS	FedRAMP Authorized	13	91

미국 정보보호 시장 동향

북미는

- 다양성, 부익부/빈익빈
  - 제로 트러스트에 근접한 고객들의 숫자도 상당수에 이른다. (Fortune 500)
  - 하지만 엄청난 수의 고객들이 단순 경계망 보안에 머물러 있다.
- 한국보다 훨씬 강력한 규제, 하지만 규제없이 들어갈 수 있는 시장도 매우 크다.
  - FedRAMP 인증 대기 2년, 비용 5억, 매월/매년 리포트 (SP의 의무 강화)
- 관리형 서비스의 천국
  - 경제적/지리적 특성에 따른 비싼 전문가, 값싼 서비스
- Cloud / SaaS 전환을 통해서
  - 자연스럽게 Zero Trust가 성숙
  - 데이터 학습을 통한 AI 기반 보안기술 발전
- 활성화된 연동 생태계
  - 보안업체 간의 인적 커넥션, 동시에 다수의 연동을 진행할 수 있는 기업의 규모/투자, 해외 엔지니어링 리소스 활용 (IT 개발 확장성)

한국은

- Zero Trust를 구현하기 위한 Point 솔루션은 그 어느 나라 보다 잘 갖추어져 있다. 하지만 그 제품 간의 연동성이 너무 부족하다.
  - 제품/문서/API 비공개, RFP 상에서 개방성에 대한 요구 필요
- 많은 기능, 복잡성 (UX만 잘 다듬으면 이것이 장점일수도)
- IT 인프라 낙후. On-Prem 중심, Cloud/Wireless/Remote 시장의 부재
  - 글로벌 기준의 제품을 만들고 싶어도 팔 곳이 없다. (Chasm 상태)
  - AI 학습을 위한 데이터확보 불가

03.

RSAC 2025
Many Voices. One Community.

RSA Conference 2025

Identity Centric

Authentication

- MFA
- Passwordless (Passkeys) 급속 확산

SSO (Single-Sign-On)

- SaaS의 대중화 다양화
- 계정관리의 어려움 해소

Authorization

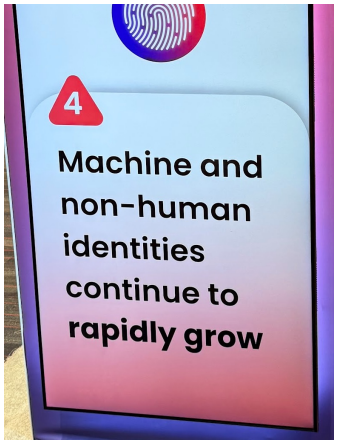
- 인증 과정에서 제로트러스트 구현에 필요한 최소권한 부여
- RBAC (Role) 에서 ABAC (Attribute) 으로 전환

Governance

- Identity 관리체계의 개선이 필요
- 슈퍼관리자에 의한 단일관리체계 -> 커뮤니티 기반 관리체계

Non-Human Identity

- 사람이 아닌 기기에 대한 인증 (Workload, IoT, AI Agent)



Cloud Security

CNAPP

- 기존 On-Prem의 파편화된 보안체계가 아닌 데이터 부터 접근제어까지 하나의 플랫폼으로 운영 효율성 극대화
- CSPM, CWPP, CIEM, Container, IaC, API, Data, Runtime Protection, Threat Detection, Compliance, Report

DevSecOps

- 개발팀과 보안팀의 단절이 큰 문제로 대두
- 개발(Development), 보안(Security), 운영(Ops)을 결합하여 보안을 개발 생명주기 초기에 내재화

Google의 Wiz 인수

- $3.2B 구글의 인수금액 사상 최대규모
- Cloud 시장 주도권 쟁탈을 위한 승부수
- 멀티클라우드를 지원하고 데이터레벨까지 억세스 가능한 플랫폼
- 엔터프라이즈 데이터에 대한 학습기반 마련

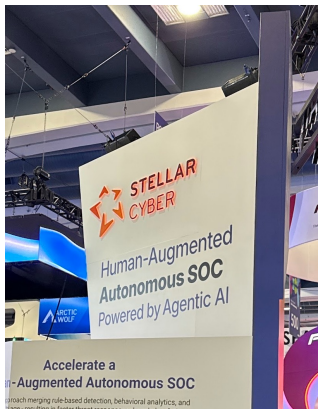
Autonomous SOC (Security Operation Center)

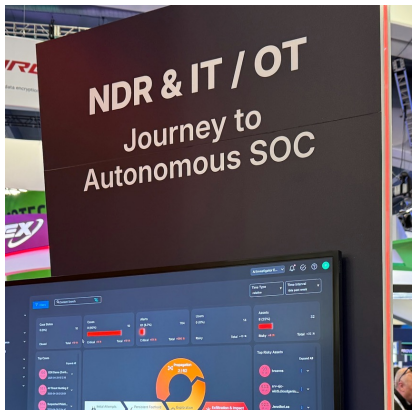
정책수립 및 집행

- 기존의 보안정책은 사람이 수립하고 UI를 통해서 관리자가 설정
- 제로트러스트 시대에는 사람이 모든 정책을 미리 수립할 수 없음
- Policy as Document
- Policy as Code (Rego, Cedar)
- Policy as AI
- 이런 보안정책을 컨설팅, 수립, 관리 해줄 MSSP가 보안시장을 주도

사고조사

- 사고조사에 필요한 분석을 사람이 손으로 하는것에 한계
- 정형 데이터, 로그 데이터를 AI/ML이 분석하기 쉬운 형태로 전환
- 온톨로지, Knowledge Graph, Vector DB, LLM 연결
- 이런 작업을 대신해줄 MSSP가 보안시장을 주도

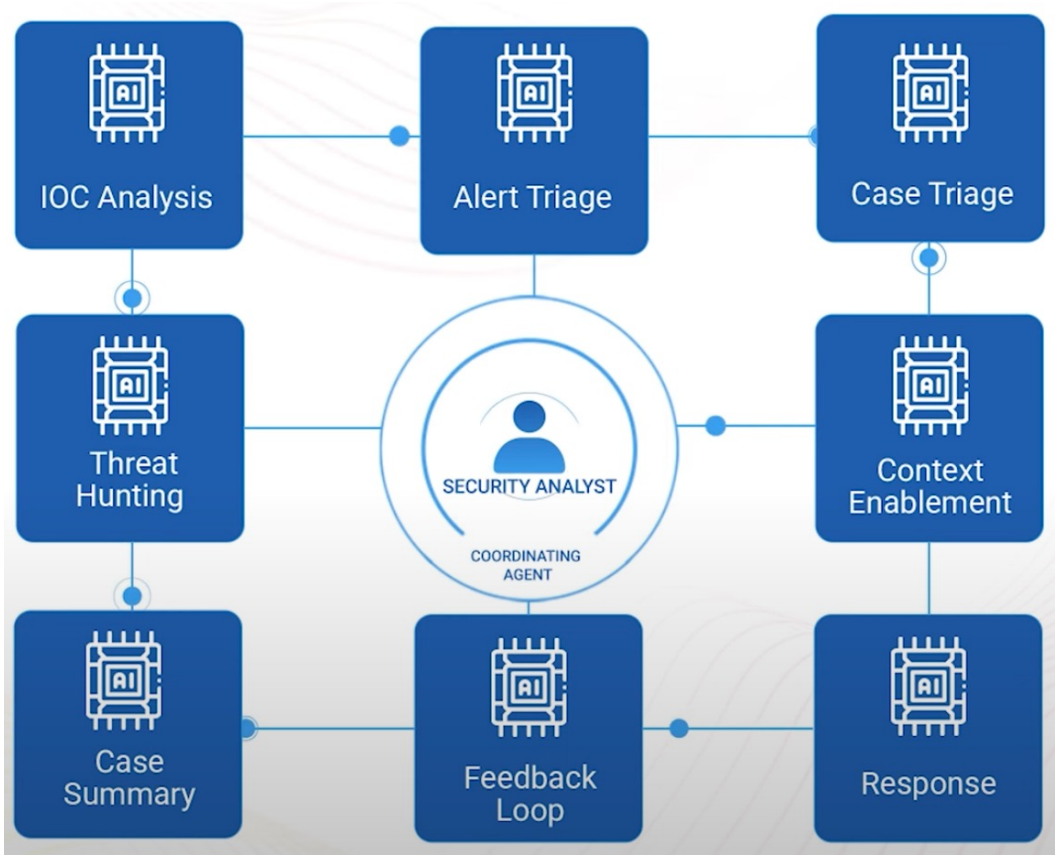




Agentic AI

Human-Augmented Autonomous SOC

- 악성파일 탐지, 비정상 행위 탐지, 오탐제거, 피싱탐지등 다양한 역할
- 하지만 사람의 개입이 필요함.



통합 보안 플랫폼 기업, 지니언스.

THANK YOU :)

Genians