5min

Cloud Breach

DigitalForensic Track
김태룡

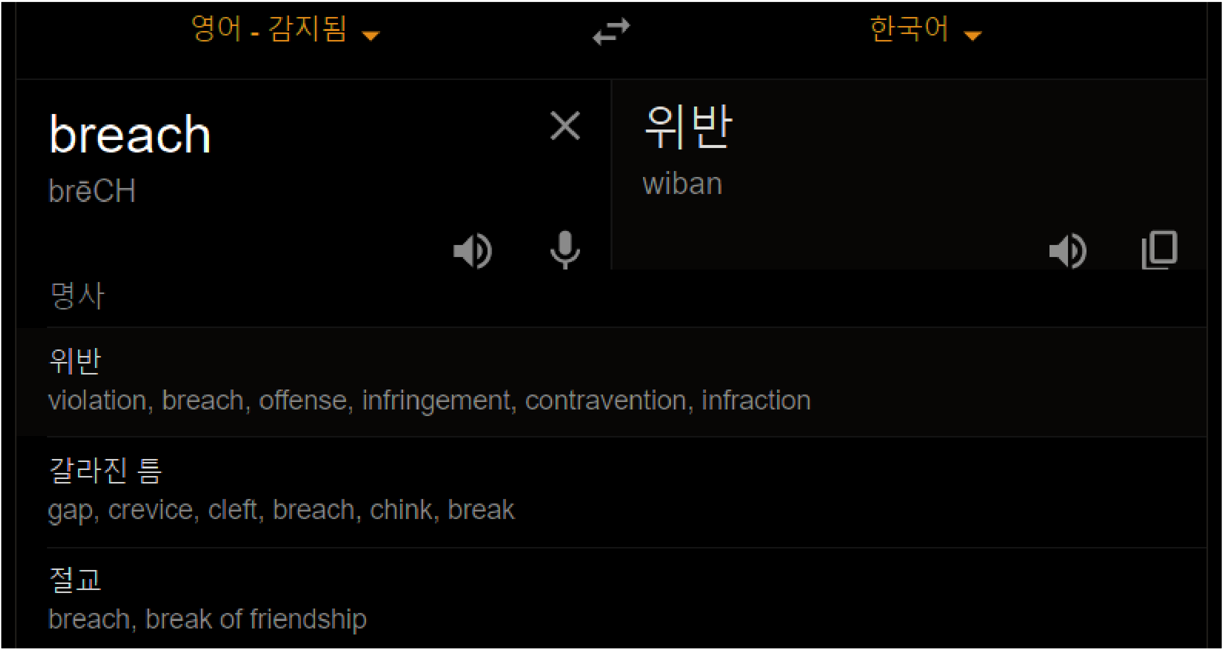
INDEX

01. Breach

02. Cases - Data Breach

03. Cases - Cloud Breach

Breach



breach
brēCH

위반
wiban

명사

위반
violation, breach, offense, infringement, contravention, infraction

갈라진 틈
gap, crevice, cleft, breach, chink, break

절교
breach, break of friendship

???

5min Cloud Breach

Breach

Don’t Think About Translation

Breach

BreachBreachBreachReachReachReachReech
ReechReechLeechLeechLeech

Leech

Breach

Data Breach

Cloud Breach

Data in company

Cases - Data Breach

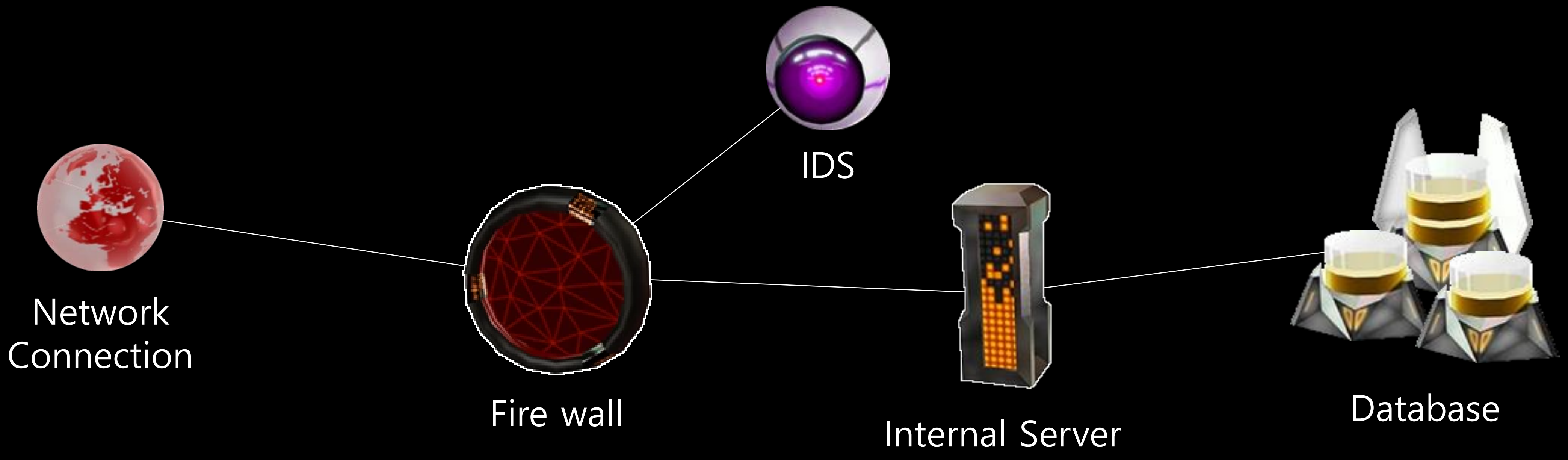
Target	Yahoo	Marriott Internationa	Adult Friend Finder
When	2013 ~ 2014	2014 ~ 2018	2016.10
Stolen	3 Billion user accounts	500 Million customers	412 Million accounts
Misconfigured	Spear-phishing	Spear-phishing	Local File Inclusion (LFI)
Attack Scenario	Send phishing mail ▶ Backdoor ▶ DB copy ▶ MD5 crack	Send phishing mail ▶ MimiKatz&RAT(Get user account) ▶ DB Query	Command Injection ▶ Access accounts DB
Detected	FBI	Internal investigation (Not discussed in detail)	Researcher who goes by the handle 1x0123
Response	Advised change password	Engaged leading security experts	Hire FireEye to help with the investigation
Remediated	Change password	WebWatcher Enrollment	Use Salted Hash

https://www.csoonline.com/article/2130877

Data in company

Cases - Data Breach

(This is just example. It may differ from the actual.)



Data in cloud service

Cases - Cloud Breach

Target	Instagram (Chtrbox)	Capital One	Autoclerk
When	2020.05.20.	2020.07.29.	2020.09.13.
Stolen	49 Million records	0.8 Million Account (1Million GovernmentID)	1 Million booking reservations (179GB)
Misconfigured	AWS password policy	Network separation	Unsecured Elasticsearch DB
Attack Scenario	Access to DB that none password policy	Access with TOR ▶ Get Access data in EC2 Metadata Service ▶ Breach AWS S3	Unknwon (Because not discovered yet)
Detected	Security researcher Anurag Sen	Email "There appears to be some leaked s3 data of yours in someone's github"	vpnMentor
Response	Configuration Vulnerability Fix		
Remediated	Instagram API Limit	-	-

https://www.lacework.com/top-cloud-breaches-2019/

Data in cloud service

Cases - Cloud Breach

Cloud Configuration

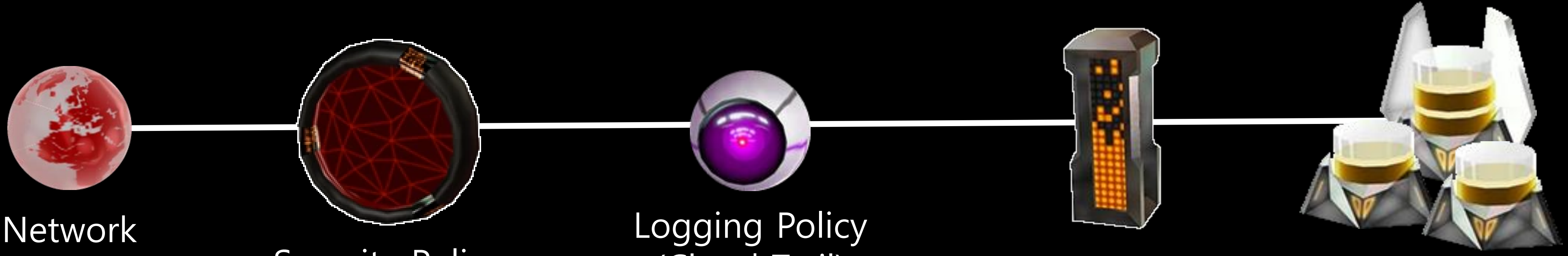
Data in cloud service

Cases - Cloud Breach

(This is just example. It may differ from the actual.)

Cloud Configuration

Safety



Network Connection

Security Policy (WAF & Shield)

Logging Policy (Cloud Trail)

Hosting (EC2)

Database (RDS)

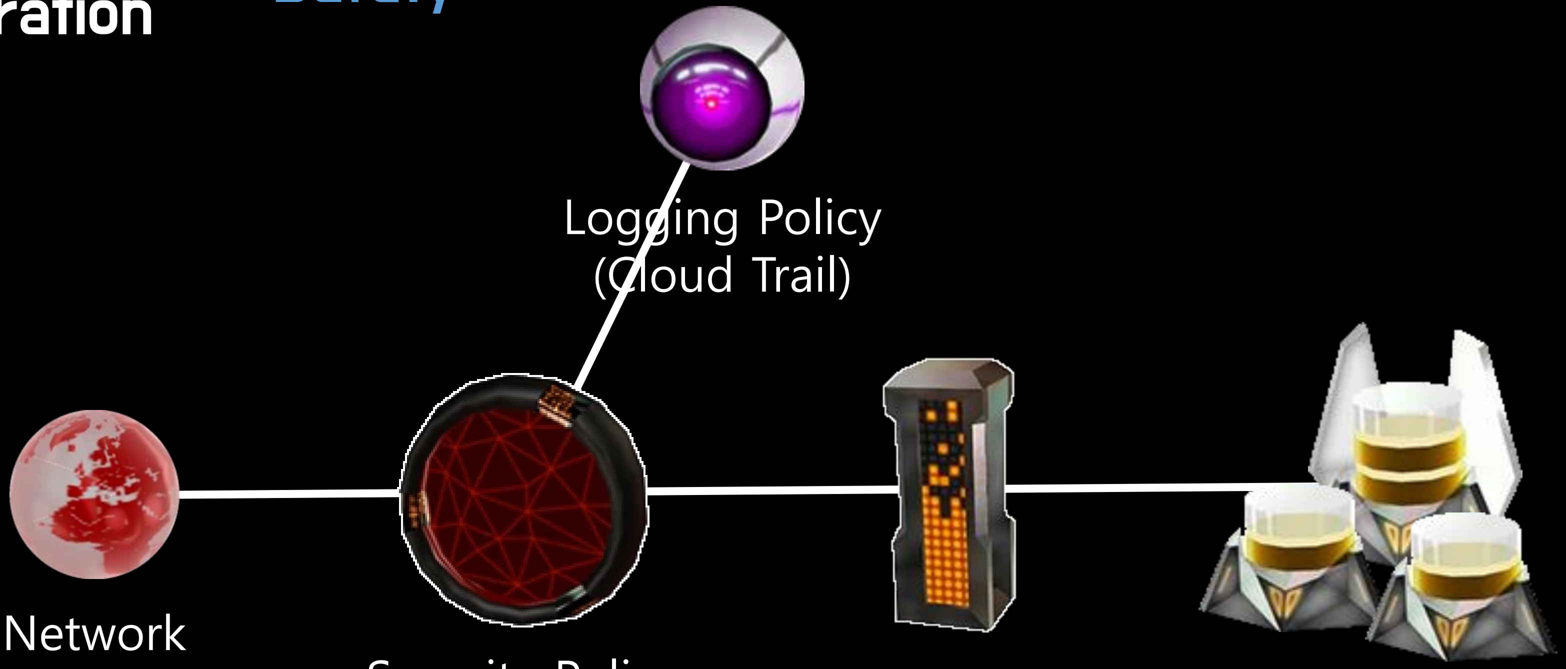
Data in cloud service

Cases - Cloud Breach

(This is just example. It may differ from the actual.)

Cloud Configuration

Safety



Logging Policy
(Cloud Trail)

Network
Connection

Security Policy
(WAF & Shield)

Hosting
(EC2)

Database
(RDS)

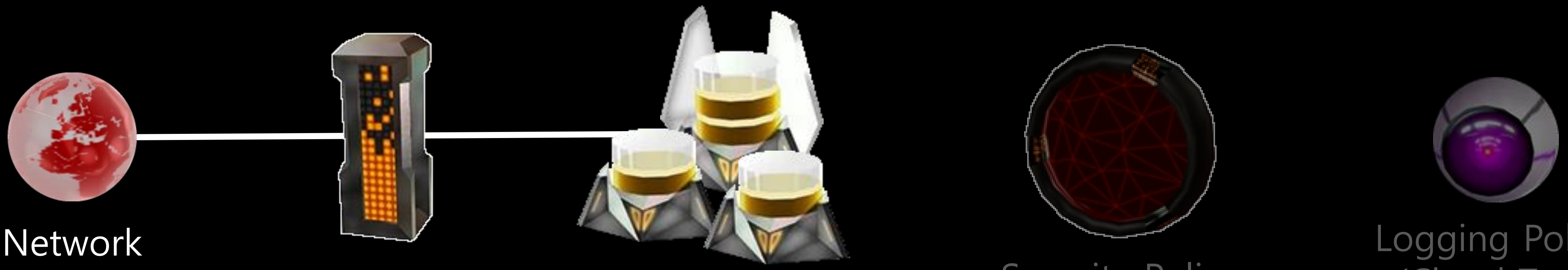
Data in cloud service

Cases - Cloud Breach

(This is just example. It may differ from the actual.)

Cloud Configuration

Vulnerable



Network Connection

Hosting (EC2)

Database (RDS)

Security Policy (WAF & Shield)

Logging Policy (Cloud Trail)

Thankyou

Image Source : Hackers (Android)