



Check Point®
SOFTWARE TECHNOLOGIES LTD

GEN V

5세대 사이버 보안과 위협징후 분석을 통한 선제적 보안

한 승 수 | 보안 컨설턴트
체크포인트 코리아

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  CHECK POINT
INFINITY

CLOUD • MOBILE • THREAT PREVENTION

사이버 보안분야에서 어떤일이 일어나고 있을까요?

2017년의 사이버 보안이 시사하는 것들



Check Point
SOFTWARE TECHNOLOGIES LTD

WannaCry

99개 국가에 걸쳐 수 천개 기업

French-elections

BadRabbit

NSA

Yahoo

wannaCry

NotPetya

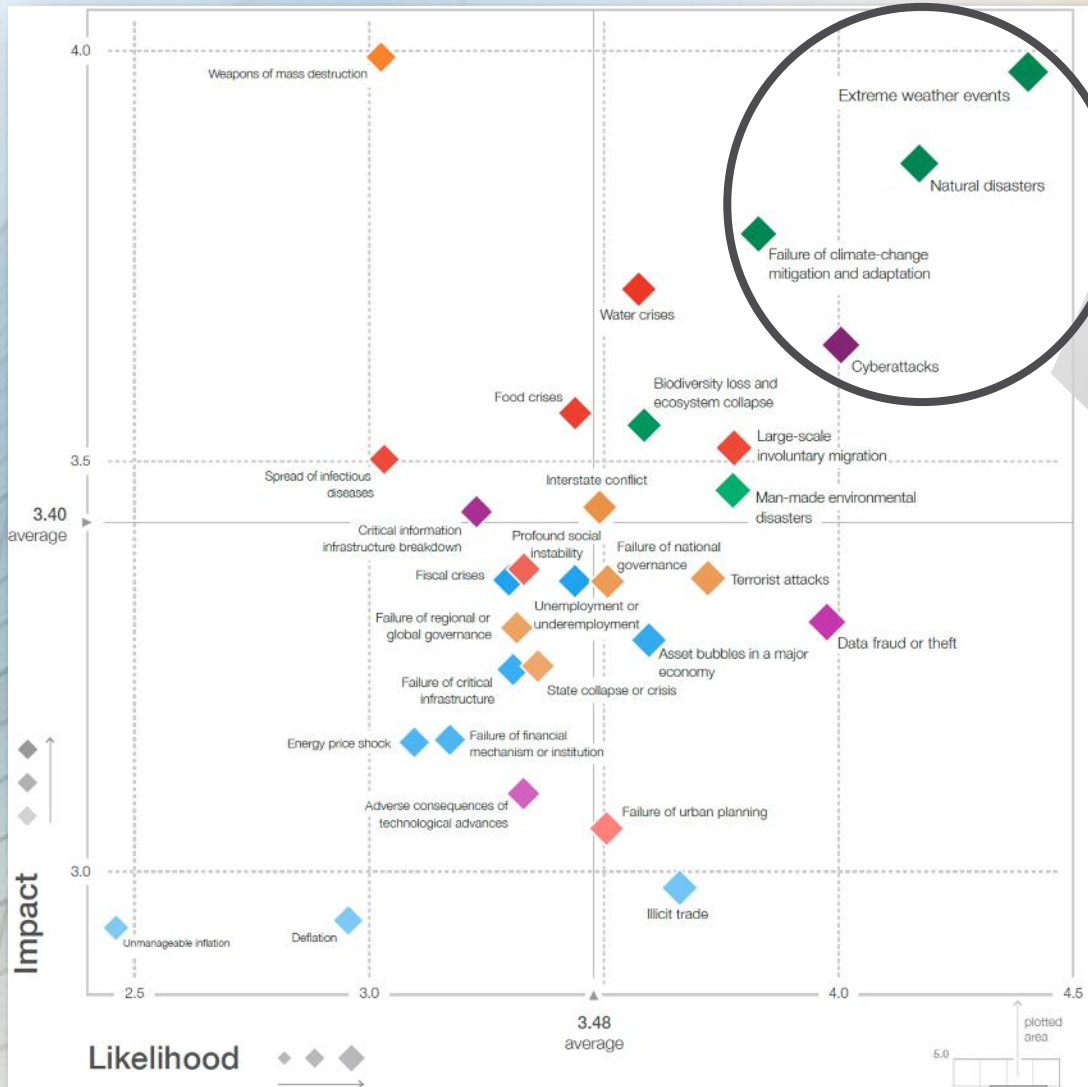
wannaCry

EQUIFAX

NotPetya

한 국가를 전체적으로 다운시켰으며 60개 이상국가에 영향

2018년 글로벌 리스크 리포트 - 세계경제포럼



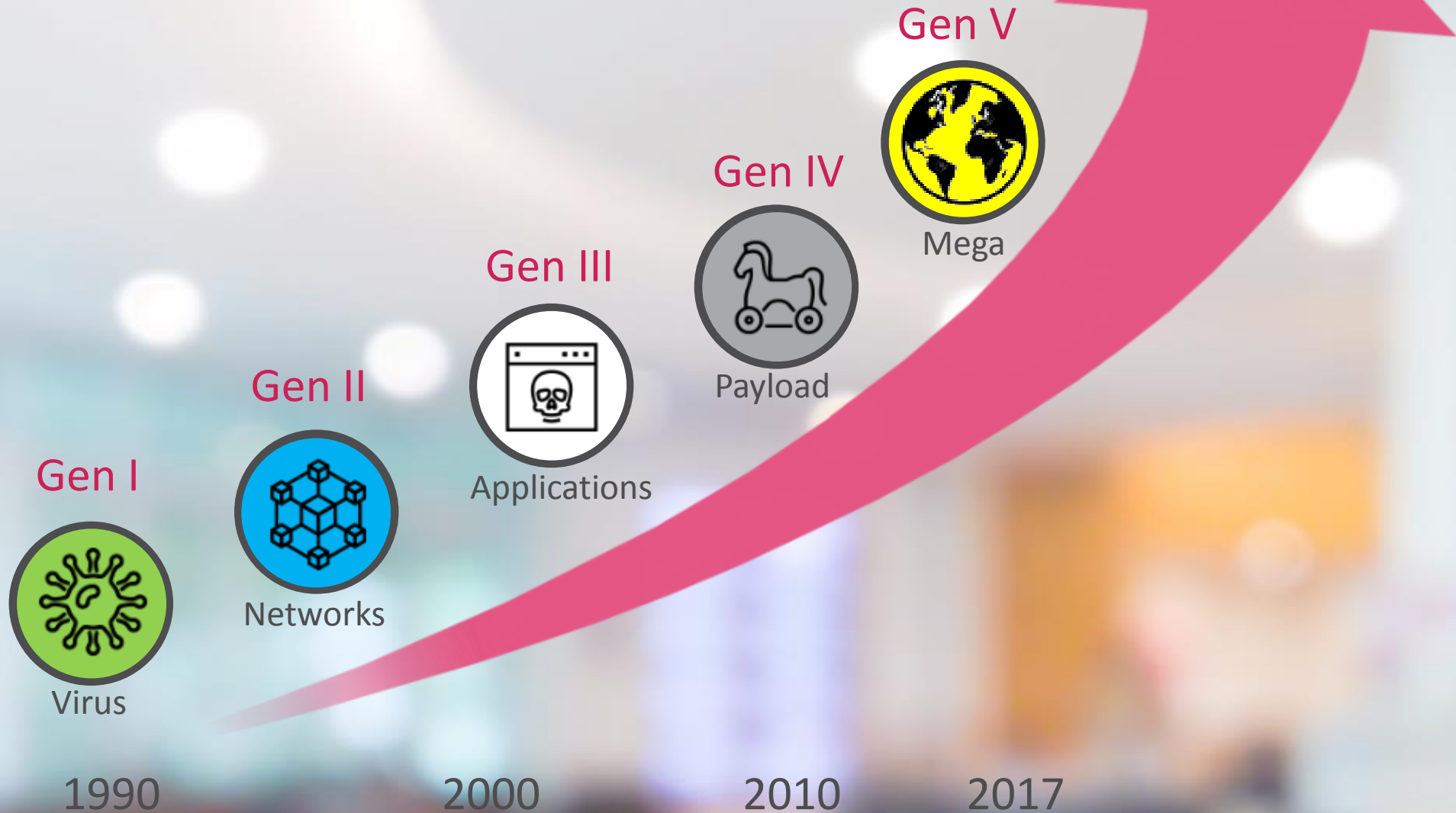
Top 5 Global Risks in Terms of Likelihood

	2016	2017	2018
1st	Large-scale involuntary migration	Extreme weather events	Extreme weather events
2nd	Extreme weather events	Large-scale involuntary migration	Natural disasters
3rd	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
4th	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
5th	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

우리는 **변곡점**에 다달았습니다!



Check Point
SOFTWARE TECHNOLOGIES LTD



사이버 공격의 세대구분 및 특징



각 세대의 공격과 방어

Gen I

100%
of
businesses

1980년대 후반
PC attacks

The Anti Virus

Gen II

100%
of
businesses

1990년대 중반
인터넷으로 부터의 공격

The Firewall

Gen III

50%
of
businesses

2000년대 초반
어플리케이션의 취약점에 대한
익스플로잇

Intrusion
Prevention (IPS)

Gen IV

7%
of
businesses

2010년대
Polymorphic (형태가 바뀌는)
Content

SandBoxing
and Anti-Bot

우리는 어디에 있을까요?



Check Point
SOFTWARE TECHNOLOGIES LTD

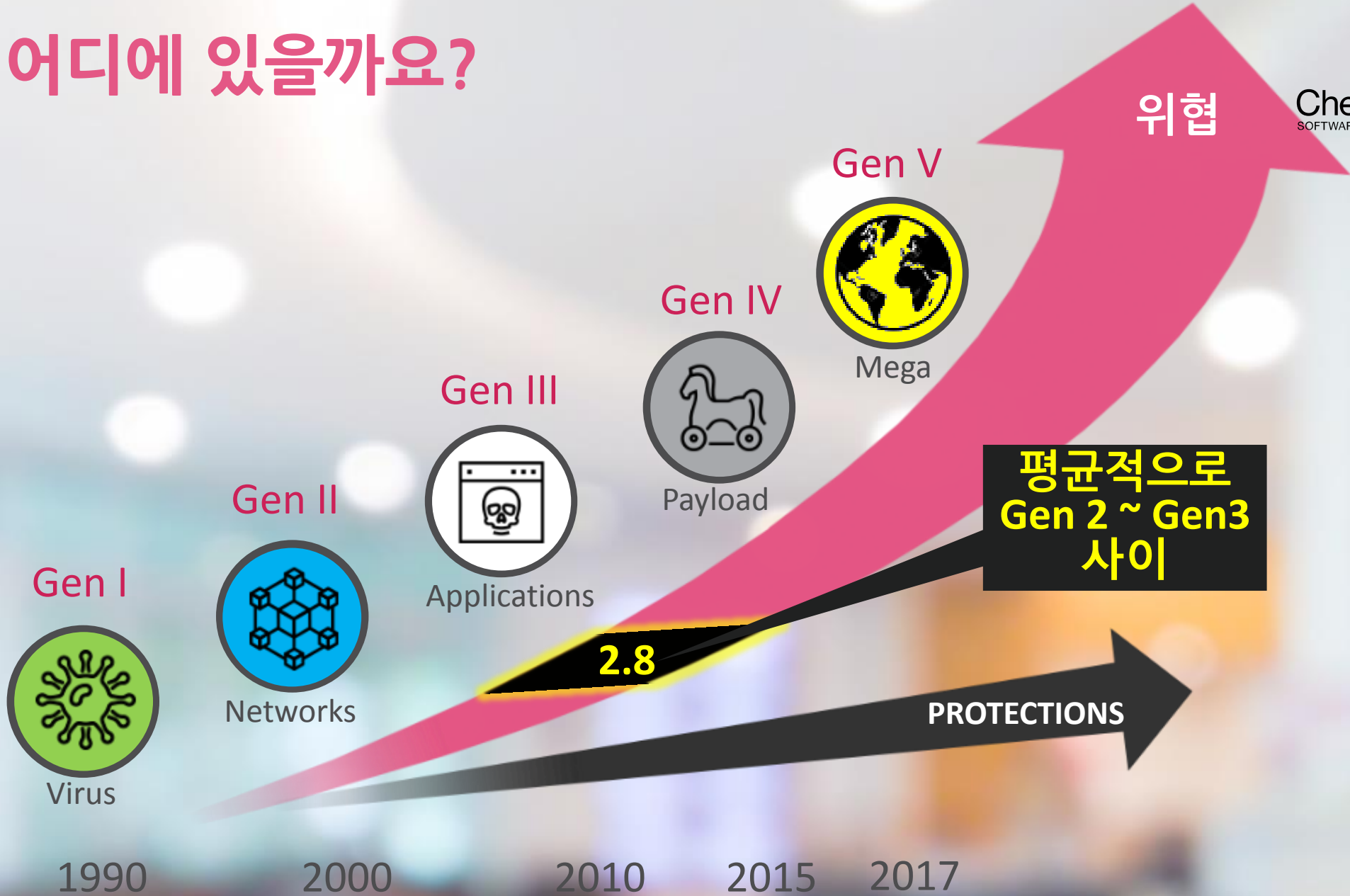
GRADE V

GRADE IV

GRADE III

GRADE II

GRADE I



위협

Gen V



Mega

Gen IV



Payload

Gen III



Applications

Gen II



Networks

Gen I



Virus

1990

2000

2010

2015

2017

PROTECTIONS

평균적으로
Gen 2 ~ Gen3
사이

2.8

2018 – GEN V 사이버 공격



Check Point
SOFTWARE TECHNOLOGIES LTD

대규모 (across country and industry)

멀티-벡터 (network, cloud, mobile)

정부기구가 후원하는 수준의 기술활용



GEN IV 방어는 충분치 않습니다!



Check Point
SOFTWARE TECHNOLOGIES LTD

Gen IV



PAYLOAD

2010 -
Polymorphic Content

SandBoxing
and Anti-Bot

차단기반의 방어
(탐지에 그치지 않는)

실시간으로 동작

가장 약한 부분인 클라우드와 모바일을
포함하는 보안

MEGA ATTACK 시대를 대비하는
GEN 5 PROTECTION을 소개합니다

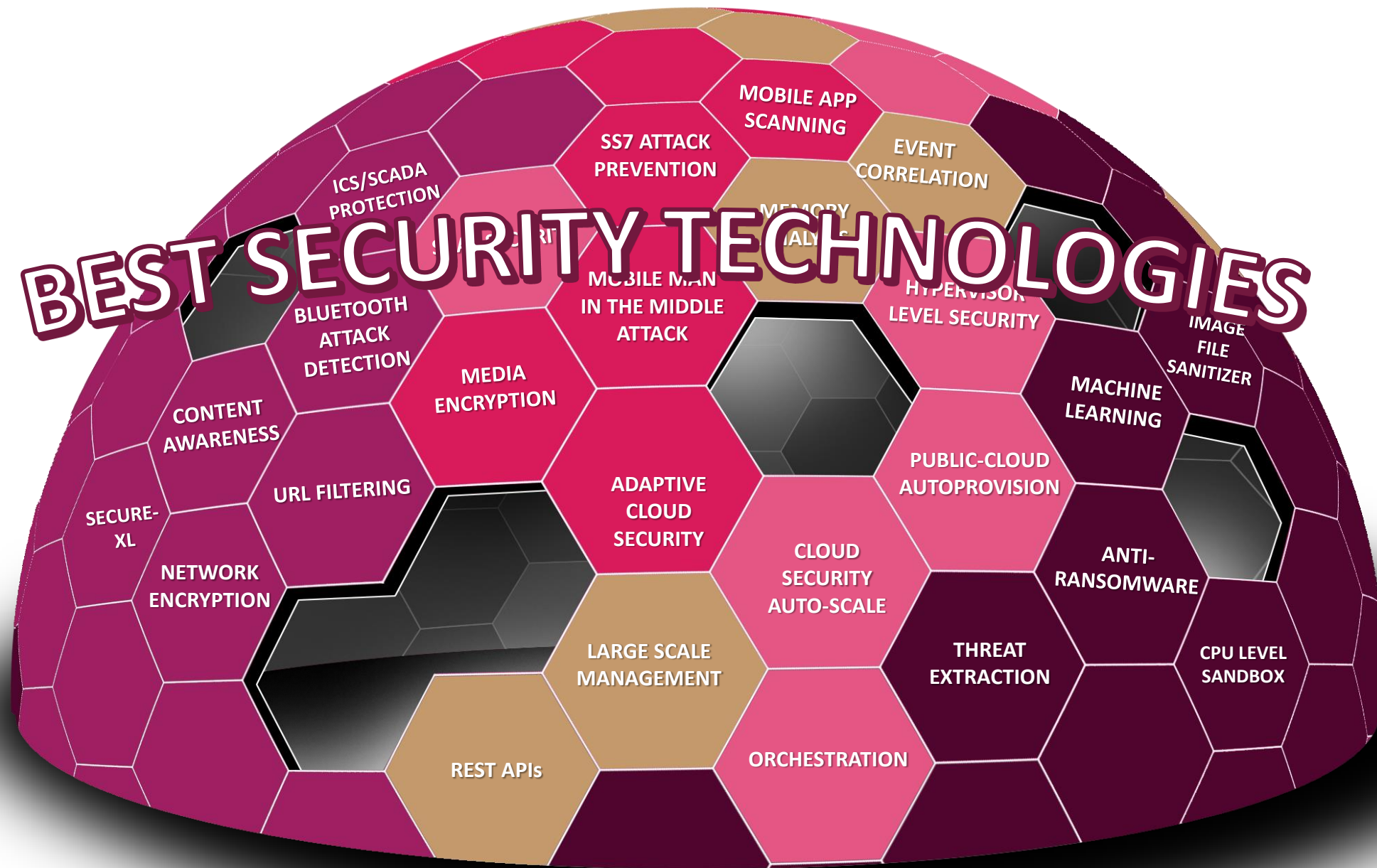


Check Point®
SOFTWARE TECHNOLOGIES LTD

GEN 5

어떤 요소들이 필요할까요?





GEN V를 실현하기



Check Point
SOFTWARE TECHNOLOGIES LTD



GEN V



CHECK POINT
INFINITY

WELCOME TO THE FUTURE OF CYBER SECURITY

©2018 Check Point Software Technologies Ltd.

우리가 어떻게 **GEN V**
보안으로 나갈 수 있을까요?

우리는 다양한 보안 기술이 필요 합니다



Check Point
SOFTWARE TECHNOLOGIES LTD



우리는 다양한 보안 기술이 필요 합니다



Check Point
SOFTWARE TECHNOLOGIES LTD

CYBERscape: Q1 2018

The image displays a comprehensive grid of cybersecurity vendors, categorized into 18 distinct security domains. Each domain is represented by a box containing logos of companies that specialize in that area. The domains include:

- Network & Infrastructure Security:** Includes vendors like Palo Alto Networks, Cisco, Fortinet, and Symantec.
- Web Security:** Includes vendors like Akamai, Cloudflare, and Sucuri.
- Endpoint Security:** Includes vendors like McAfee, Symantec, and Trend Micro.
- Application Security:** Includes vendors like Veracode, Snyk, and Checkmarx.
- MSSP:** Includes vendors like IBM, Verizon, and Tenable.
- Data Security:** Includes vendors like McAfee, Symantec, and Trend Micro.
- Mobile Security:** Includes vendors like Symantec, McAfee, and Trend Micro.
- Risk & Compliance:** Includes vendors like Delve, RiskSense, and Tenable.
- Security Operations & Incident Response:** Includes vendors like Splunk, Palo Alto Networks, and Fortinet.
- Threat Intelligence:** Includes vendors like Anomali, Recorded Future, and Intel.
- IoT:** Includes vendors like Cisco, Intel, and Microsoft.
- Identity & Access Management:** Includes vendors like Okta, Duo, and Saviom.
- Security Incident Response:** Includes vendors like Palo Alto Networks, Fortinet, and Trend Micro.
- Digital Risk Management:** Includes vendors like BrandProtect, Crisp, and Digital Shadows.
- Security Consulting:** Includes vendors like Accenture, Deloitte, and IBM.
- Blockchain:** Includes vendors like Chain, Guardtime, and NuID.
- Fraud & Transaction Security:** Includes vendors like Sift Science, Sifted, and Sift.
- Cloud Security:** Includes vendors like Palo Alto Networks, Fortinet, and Trend Micro.

체크포인트 인피니티는 가능합니다



Check Point
SOFTWARE TECHNOLOGIES LTD



CHECK POINT INFINITY

THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

Endpoint
Detection
& Response

Threat
Extraction

Human
Behavioral
Analytics

DGA
Detector

Data
Encryption



Check Point®
SOFTWARE TECHNOLOGIES LTD



CHECK POINT INFINITY

네트워크, 클라우드 및 모바일 환경을
아우르는 최초의 통합형 보안으로 가장 높은 수준의
위협 방지 기능 제공



Check Point®
SOFTWARE TECHNOLOGIES LTD



CHECK POINT INFINITY



클라우드



모바일



위협 방지
(Threat Prevention)



통합 시스템



Check Point

SandBlast[™]

**ZERO-DAY
PROTECTION**

**엔터프라이즈를 위한
진보된 위협 차단 플랫폼**



샌드박스

THREAT EMULATION



특화된 탐지 엔진 30개

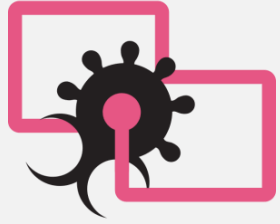
알려지지 않은 말웨어나
제로데이 공격들에 대한
탐지 및 차단 제공

무해화

THREAT EXTRACTION



지연없이 재구성된 안전한
파일을 전달



샌드박스 - CPU LEVEL 탐지



CPU 레벨에서 이상행위를 탐지하여 익스플로잇 시도를 차단

말웨어가 다운로드 되기 전에
그리고 우회 코드가 실행되기 전에..



무해화

THREAT EXTRACTION

파일을 안전하게 재구성하여
제공하며, 지연 발생 없음

유입되는 문서를 깨끗히 재구성

✓ 잠재적으로 위험한 콘텐츠를 제거하거나 PDF로 변환

깨끗히 재구성된 문서는 수초내에 전달되며,
샌드박싱은 백그라운드에서 수행

에뮬레이션 결과가 “정상”인 경우
사용자가 직접 원본 파일 다운로드 가능



첨부 파일에 대한 즉각적인 보호

안전한 파일을 신속히 전달

THREAT EXTRACTION DEMO

From: Julia Reyes
To: Boaz Barzel
Cc:
Subject: ALERT!!! Skipped invoice
Message Invoice.cleaned.doc.pdf (199 KB)

완벽한 보안을 위해 PDF로
변환하거나 악성 콘텐츠를
제거한 원본 파일 형태로
제공

This email's attachments were cleaned of potential threats by Check Point Gateway.

Invoice.cleaned.doc.pdf : file(s) were successfully converted to PDF.
Click [here](#) if the original attachments are required (justification required).

Hi Boaz

Attached is invoice #4409 881.69 from May which was missing

I am out of office till next week, so I'm emailing you now to re-send
[\[Blocked Malicious URL\]](#) and complete the payment as soon as possible.

Julia Reyes / Credit Manager
Pacemaker Steel and Piping Co. Inc.
Tele: 740 247-2569
Fax: 740 247-7691

Email Secured By Check Point.

invoice.cleaned.pdf - Adobe Acrobat Pro

File Edit View Document Comments Forms Tools Advanced Win

Create Combine Lock Pen Multimedia

1 / 1

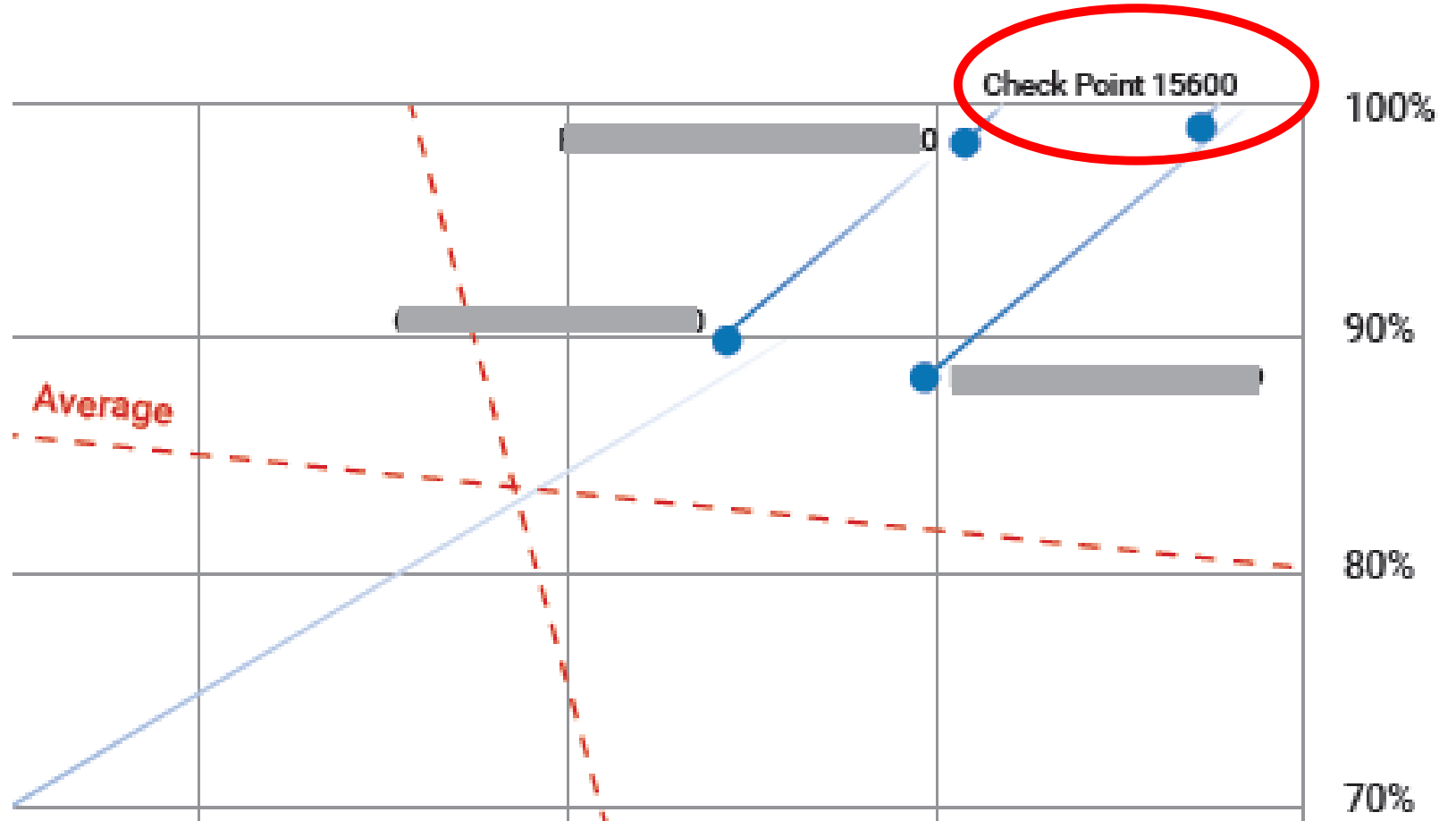
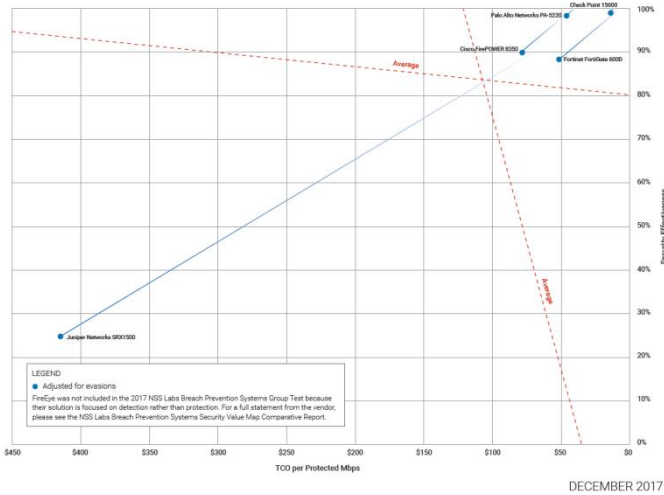
Pacemaker Steel and Piping

Tele: 740 247-2569

Fax: 740 110-7691

NSS Labs의 Breach Prevention Systems Test (2017년 12월)

Security Value Map™
Breach Prevention Systems (BPS)



- ✓ 최고의 공격차단율과 제일 적은 총 소유 비용
- ✓ 체크포인트 데이터시트 대비 3배의 성능으로 평가 (15600, 9.2G)

그리고 다음에는 어떤일이
일어날까요?



age of

THINGS



Check Point
SOFTWARE TECHNOLOGIES LTD

“컴퓨터 네트워크”를 다루는 것에
그치지 않음

모든것이 서로 연결되고, 모든것이
타겟이 됨



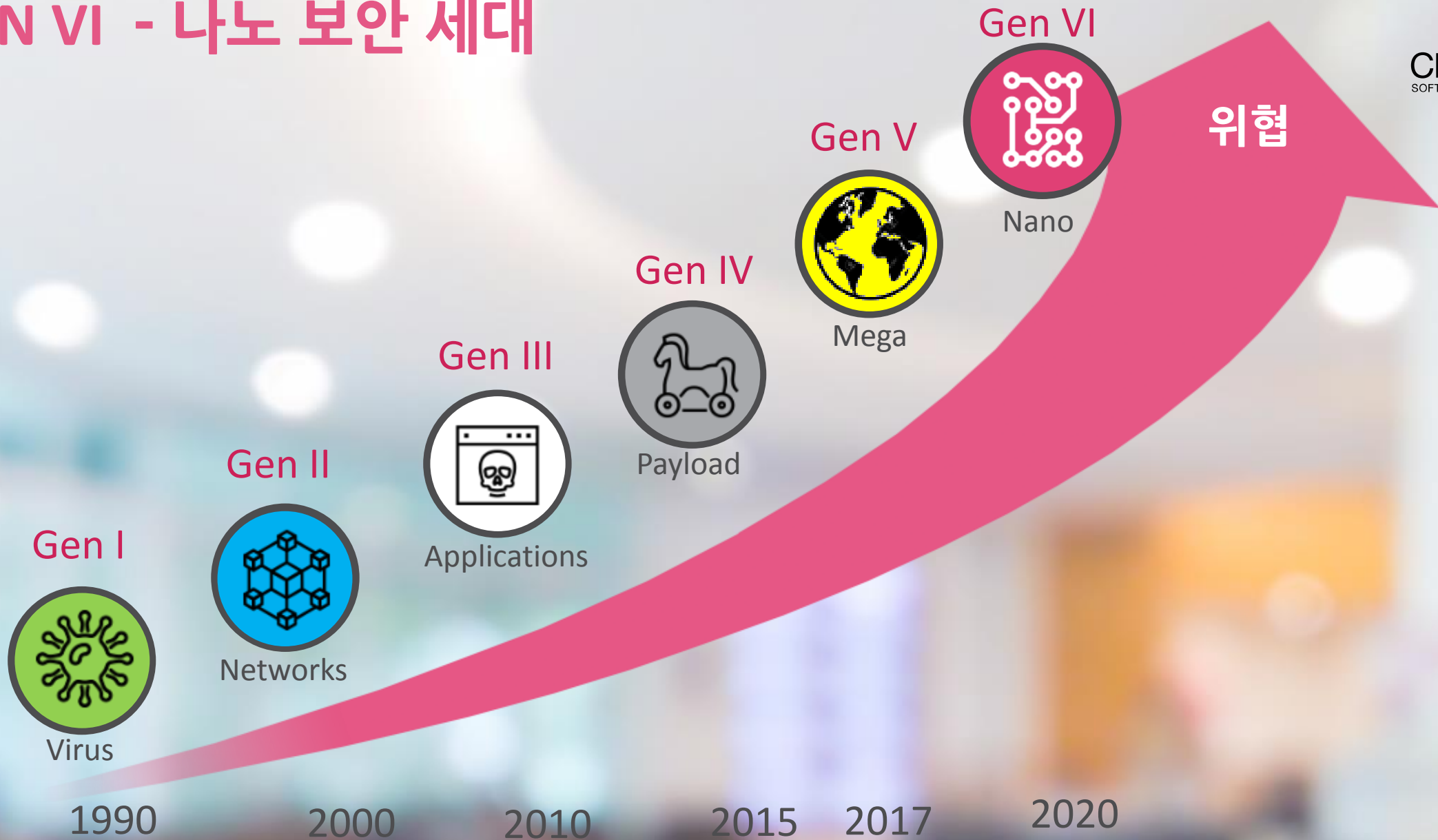
WELCOME TO THE FUTURE OF CYBER SECURITY

©2018 Check Point Software Technologies Ltd.

GEN VI - 나노 보안 세대



Check Point
SOFTWARE TECHNOLOGIES LTD



age of

THINGS



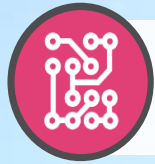
Check Point
SOFTWARE TECHNOLOGIES LTD



WELCOME TO THE FUTURE OF CYBER SECURITY

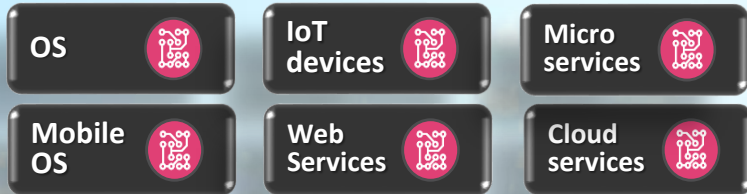
©2018 Check Point Software Technologies Ltd.

GEN VI - 나노 보안을 소개합니다



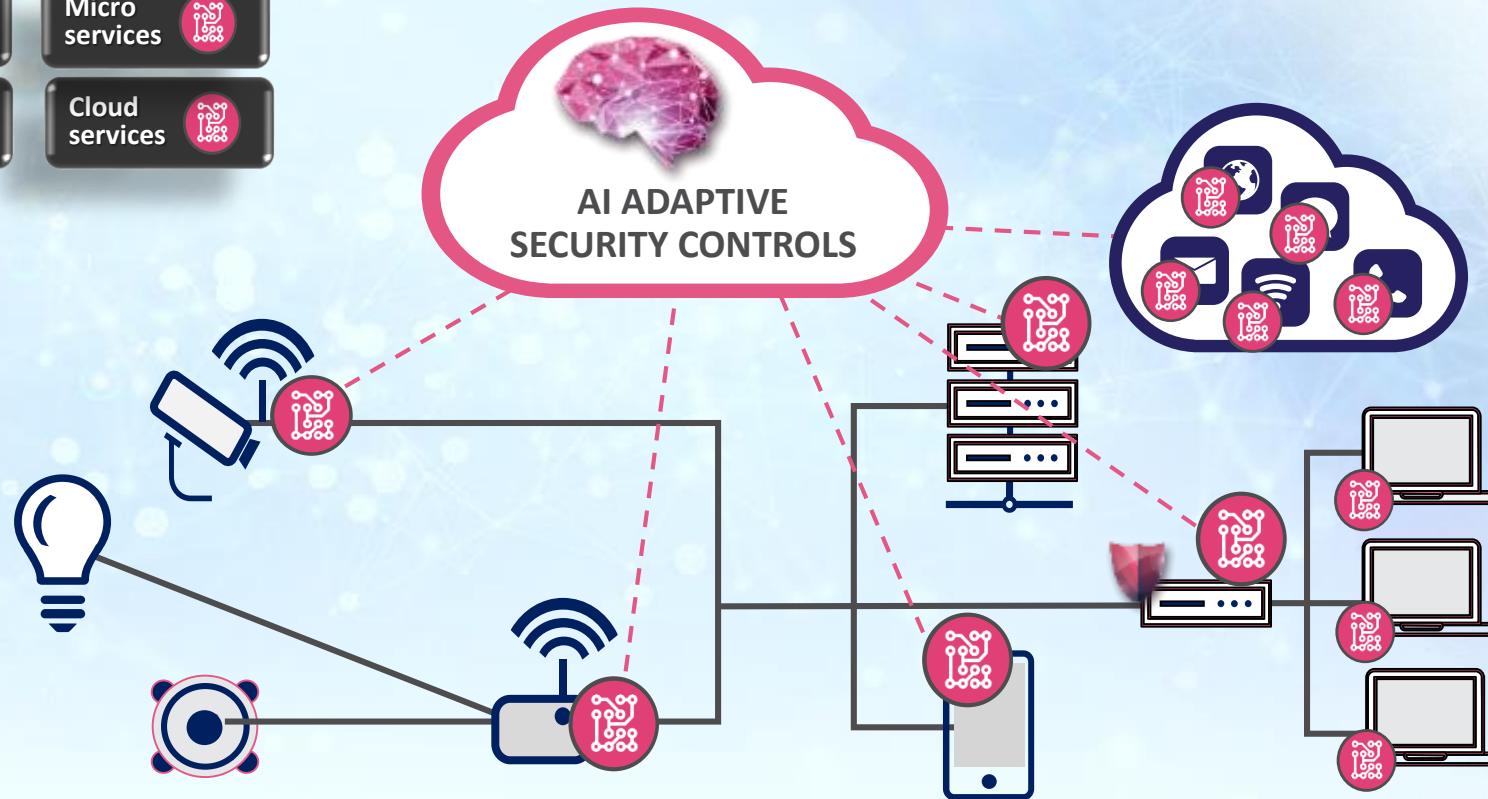
나노 에이전트

보안관련된 모든 속성을 통제하는
소프트웨어 플러그 인



인텔리전스와 컨트롤

AI에 기반한 예측 보안 지침





AI ADAPTIVE SECURITY CONTROLS

Telecom

Smart cities

cloud

Healthcare

Utilities

Smart buildings

Smart homes

Manufacturing

Automotive

Transportation

Energy

Banking

WELCOME TO THE FUTURE OF CYBER SECURITY

선제적 보안을 위한 사이버 위협 인텔리전스

클리어, 딥 & 다크 웹

클리어 웹

4 % of WWW 콘텐츠

- Searchable
- Social media

딥 웹

95 % of web 콘텐츠

- Not searchable by most engines
- Password protected content

다크 웹

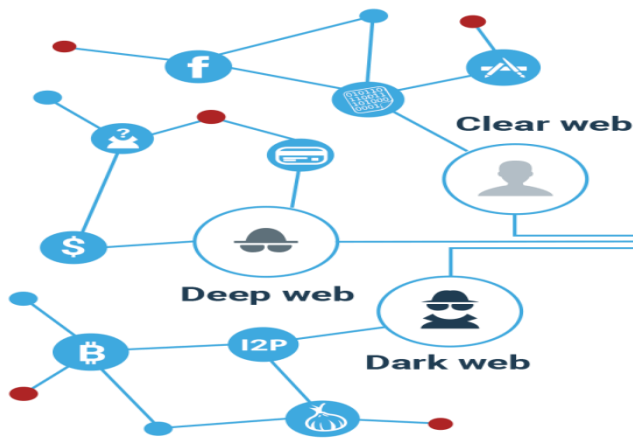
1 % of web 콘텐츠

- Home to TOR, IRCs, BitTorrent, hacker forums, C2s, and more.
- 공격이 준비되어 지고, 해킹 도구를 살 수 있으며, 정보가 거래되고, 말웨어가 개발되고 테스트되고 판매되는 곳

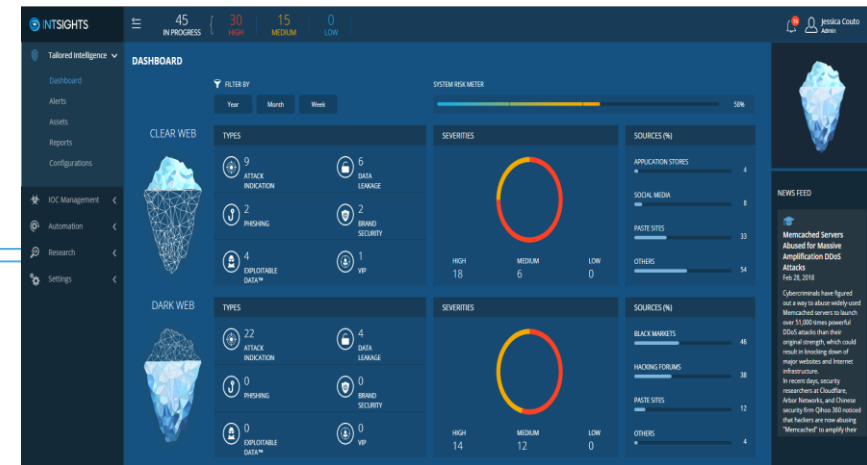


인텔리전스기반 보안

- 탐지 - Clear, Deep & Dark 웹 등 다양한 범위에 걸친 지속적인 스캐닝
- 분석 - 사이버 위협을 실시간으로 분석, 카테고리화 및 우선 순위 설정
- **경보 및 위협제거 방안**- 사이버 인텔리전스를 액션을 취할 수 있는 보안 alert로 변환하고 위협제거 방안 지원



Analysis engines

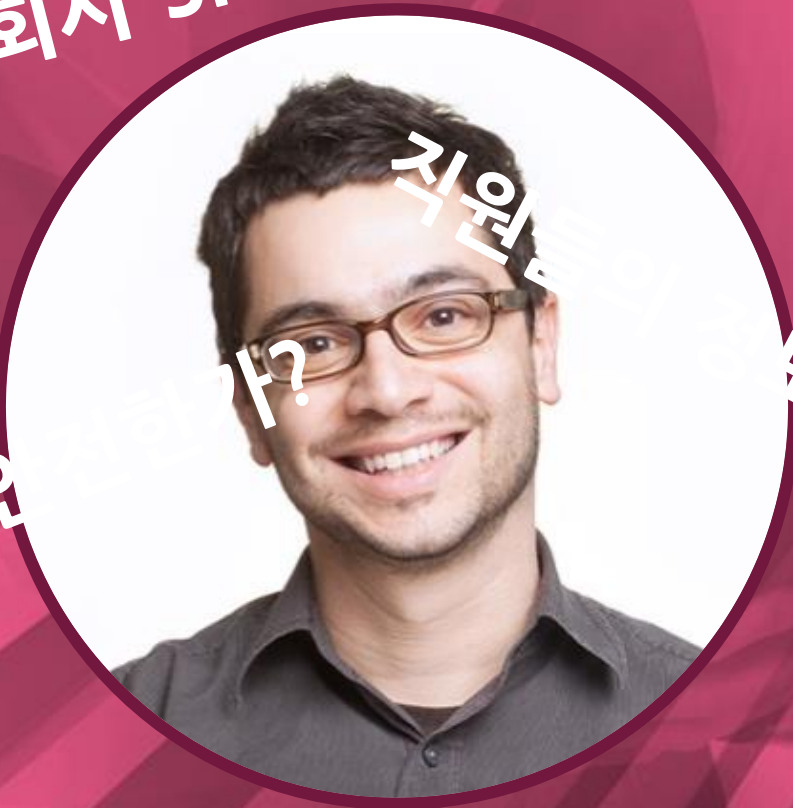


Demo - THE STORY



홍길동 - XX 금융 CSO

회사 SNS 사칭은?



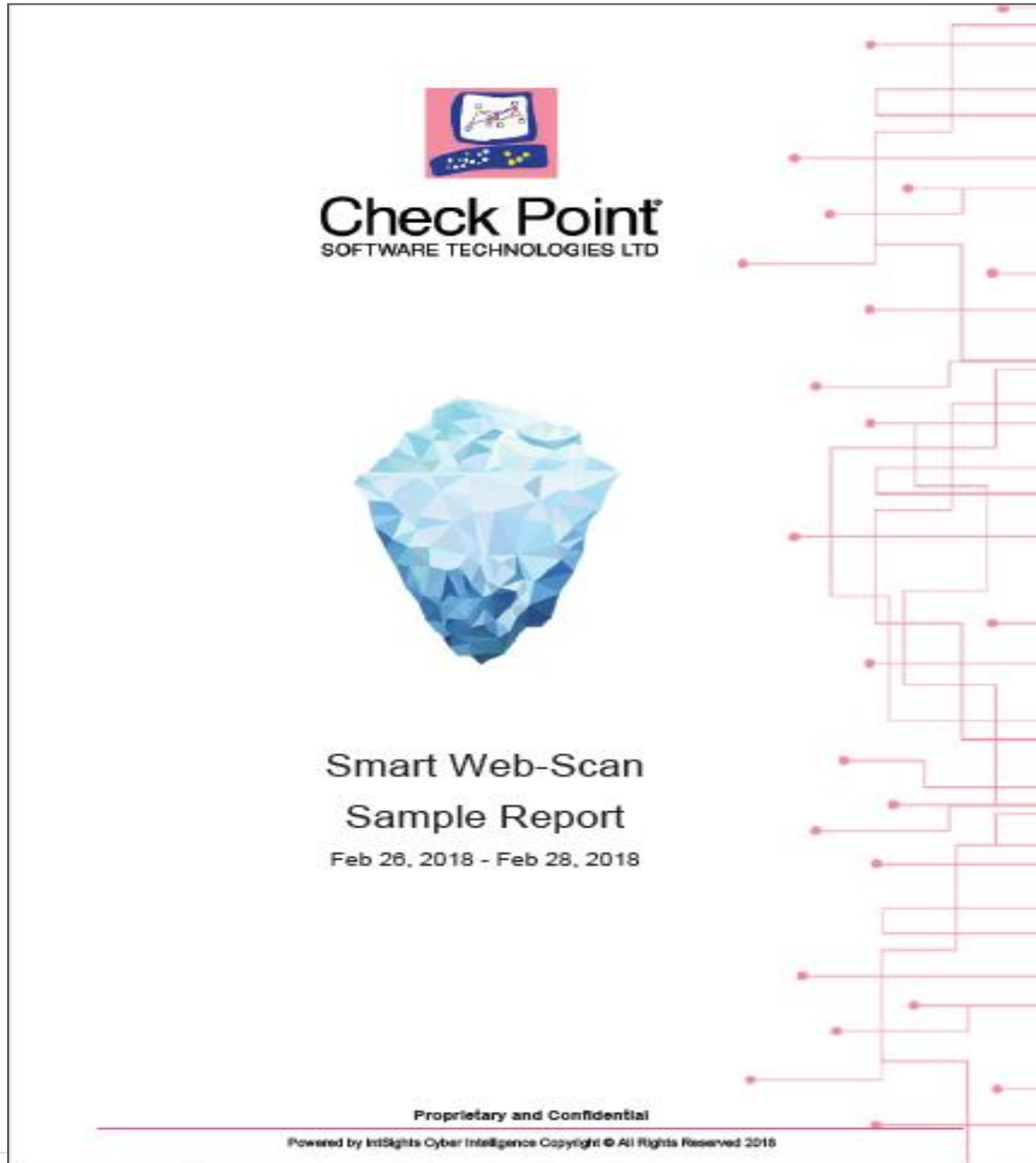
회사 웹 사이트는 인가?

직원

부유출 사례는 없나?

우리회사에 대한 공격징후는 없나?

샘플 리포트



Summary



Background

The goal of this report is to provide a clear intelligence overview of the cyber threats your company was confronting during Feb 26, 2018 - Feb 28, 2018. The intelligence findings are based on alerts that were detected and provided via the portal. We scan thousands of sources in the Dark Web (closed networks characterized by underground activities) and many more in the Clear Web (The known-to- all web accessible by regular search engine), including black markets, hacking forums, search engines, paste sites, app stores etc.

This report shows the main alerts we detected among many others.

Alert Summary

Distribution of alerts by alert types and severity levels:

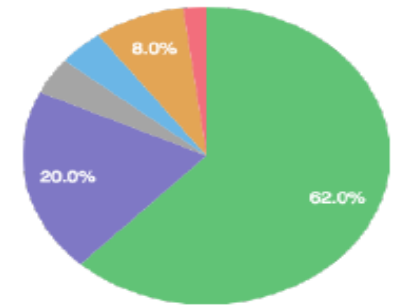
	Attack Indication	Data Leakage	Phishing	Brand Security	Exploitable Data	VIP	Total
High	18	9	1	2	1	1	32
Medium	13	1	1	0	3	0	18
Low	0	0	0	0	0	0	0
Total	31	10	2	2	4	1	50



Statistics

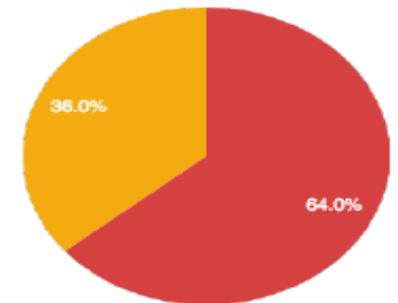
Alert Types

- Attack Indication - 31
- Data Leakage - 10
- Phishing - 2
- Brand Security - 2
- Exploitable Data - 4
- VIP - 1



Severity Levels

- High - 32
- Medium - 18
- Low - 0





Phishing

Phishing is one of the most common cyber-attacks. Since it takes advantage of the human factor it is very dangerous to any organization with any level of security. It seems that hackers take advantage of your brand in order to seduce its employees or customers to hand in sensitive information.

Highlighted Phishing alerts:

Severity	Source Date	Title	Source URL
Medium	Jan 30, 2018	Registered suspicious domain - 'int[redacted].com'	http://i[redacted]
Medium	Dec 19, 2017	Registered suspicious domain - 'in[redacted].com'	http://in[redacted]
Medium	Jun 21, 2018	Registered suspicious domain - 'in[redacted].com.au'	http://ir[redacted].com.au
Medium	Jun 21, 2018	Registered suspicious domain - 'int[redacted].de'	http://inter[redacted].de
Medium	Jun 21, 2018	Registered suspicious domain - 'int[redacted].ga'	http://ir[redacted].ga
Medium	Jun 21, 2018	Registered suspicious domain - 'in[redacted].nl'	http://inte[redacted].nl



Data Leakage

Leaked sensitive data may cause direct damage to the company. Leakage of credentials or technical data can result in a data breach, while leakage of other sensitive information can result in a direct business damage.

Highlighted Data Leakage alerts:

Severity	Source Date	Title	Source URL
Medium	Nov 09, 2016	Dark Web - 35 login credentials of employees were leaked	N/A
Low	Nov 25, 2017	1 login credentials of employee were leaked	N/A
Low	Aug 30, 2016	Dark Web - 34 login credentials of employees were leaked	N/A
Low	Jun 02, 2016	Dark Web - 5 login credentials of employees were leaked	N/A
Low	May 30, 2016	Dark Web - 1 login credentials of employee were leaked	N/A
Low	May 18, 2016	Dark Web - 21 login credentials of employees were leaked	N/A



Brand Security

Fake social media profiles and fake mobile applications can be used for social engineering against the company employees and customers, in the purpose of phishing and/or scamming activities.

Highlighted Brand Security alerts:

Severity	Source Date	Title	Source URL
High	May 28, 2018	A suspicious mobile application was detected	http://apkpure.co/%EC%9D%B8%ED%84%B0%ED%8C%8C%...
Medium	Jun 21, 2018	Suspicious Google Plus account	https://plus.google.com/109797011807038902495?...
Medium	Jun 21, 2018	Suspicious Google Plus account	https://plus.google.com/112489762697961841086?...
Medium	Jun 21, 2018	Suspicious Instagram account	N/A
Medium	Sep 12, 2017	A suspicious mobile application was detected	http://apkpure.co/it...
Medium	Jul 24, 2017	A malicious mobile application was detected	http://allfreeapk.com/



Attack Indication

Detection of upcoming cyber-attacks is crucial for effective security operations. In addition, it's important to detect the effects of past attacks, in order to understand the full scope of the damage and prepare for the next one.

Highlighted Attack Indication alerts:

Severity	Source Date	Title	Alert ID	Source URL
High	Jul 01, 2016	Company website is on an SQL Injection vulnera...	5a971afd8eceab00068c43e6	N/A
High	Invalid date	Company product was hacked	5a971afd8eceab00068c43ed	N/A
High	Jul 01, 2016	Dark Web - Company documents are offered for s...	5a971afe8eceab00068c43f4	N/A
High	Jul 03, 2016	Company employees are on a target list	5a971b0b8eceab00068c4471	N/A
Medium	Apr 13, 2017	Dark Web - Technology in use is targeted by...	5a971b318eceab00068c4599	N/A
Medium	Feb 28, 2018	Company domain is embedded in a malware code	5a971b218eceab00068c4524	N/A



VIP

VIP are main targets of hacking because of their key positions and the sensitive data they are exposed to. Also, they can be targeted by frustrated customers and past employees, who seek to protest against the company activities.

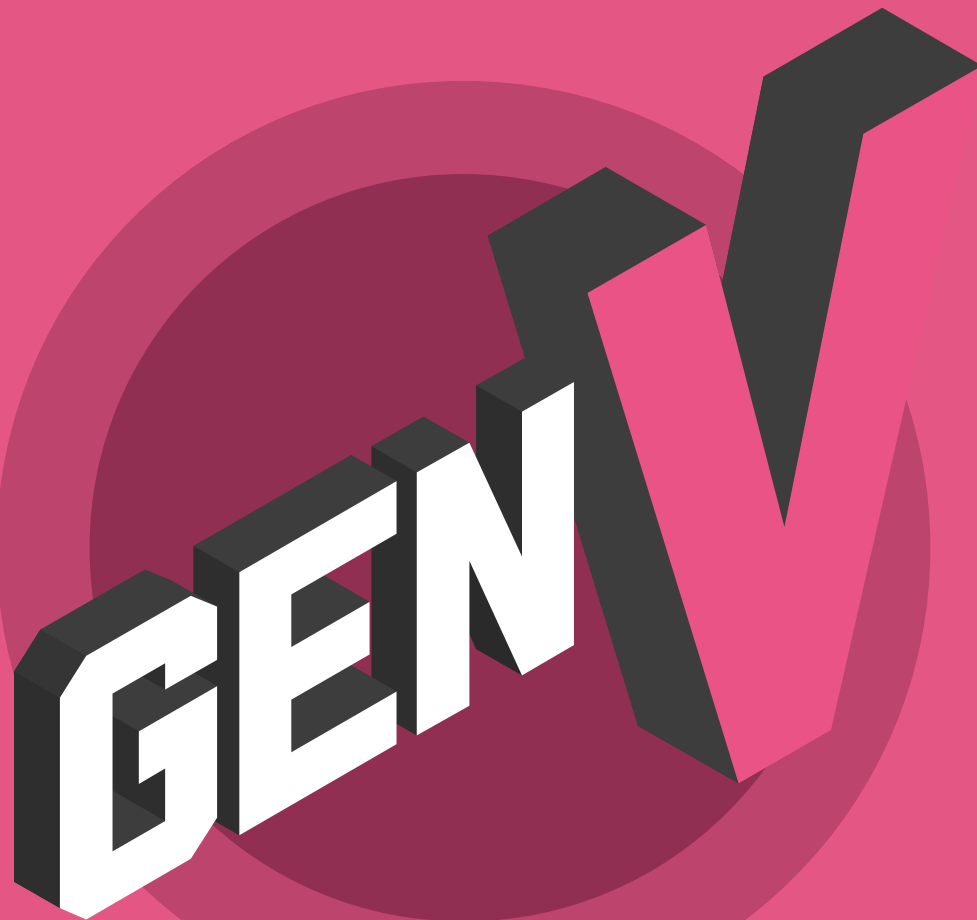
Highlighted VIP alerts:

Severity	Source Date	Title	Source URL
Medium	Nov 29, 2017	VIP - 1 login credentials of employee were leaked	N/A
Low	May 10, 2017	VIP - 1 login credentials of employee were leaked	N/A

SUMMARY

우리는 **변곡점**에 서 있습니다!





최고의 보안,
실시간 보호



CHECK POINT
INFINITY