MANDIANT
NOW PART OF Google Cloud

Global Perspective on Threat Intelligence

미디어 인터뷰 I 20 Feb, 2023

Jinsuk Oh

Head of Security Engineers, Mandiant Korea & North Asia

MANDIANT
NOW PART OF Google Cloud

Global Perspectives on Threat Intelligence

1,000명 이상의 글로벌 대형 기업 및 조직의 보안 결정권자의 위협 인텔리전스에 대한 인식, 현황 확인을 위한 설문 조사 결과 보고서

1,350

- 보안에 대한 결정권이 있는 비즈니스 및 IT리더
- 임직원 수가 1,000명 이상인 조직

3 / 13 / 18

- 북미지역, 아태지역, 유럽지역
- UK, Germany, France, Italy, Middle East, USA, Canada, Singapore, Australia, Japan, **Hong Kong**, Korea, India
- 18개 산업군 포함
  : 금융, 의료, 제조, 공공. 하이테크, 통신사, 교육, 에너지 등

- Global 응답자 1,350
- JAPAC 응답자 600
- Korea 응답자 100

- 전체 응답자 중 약 400명은 기업 이사회 임원 또는 C-레벨

- 설문은 3가지 카테고리 27개 항목으로 구성되어 진행

Q1. 조직의 고위 경영진은 귀사의 사이버 위협을 얼마나 정확하게 파악하고 있다고 생각하십니까?

67 %(Global)
63 %(JAPAC)
36 %(Korea)

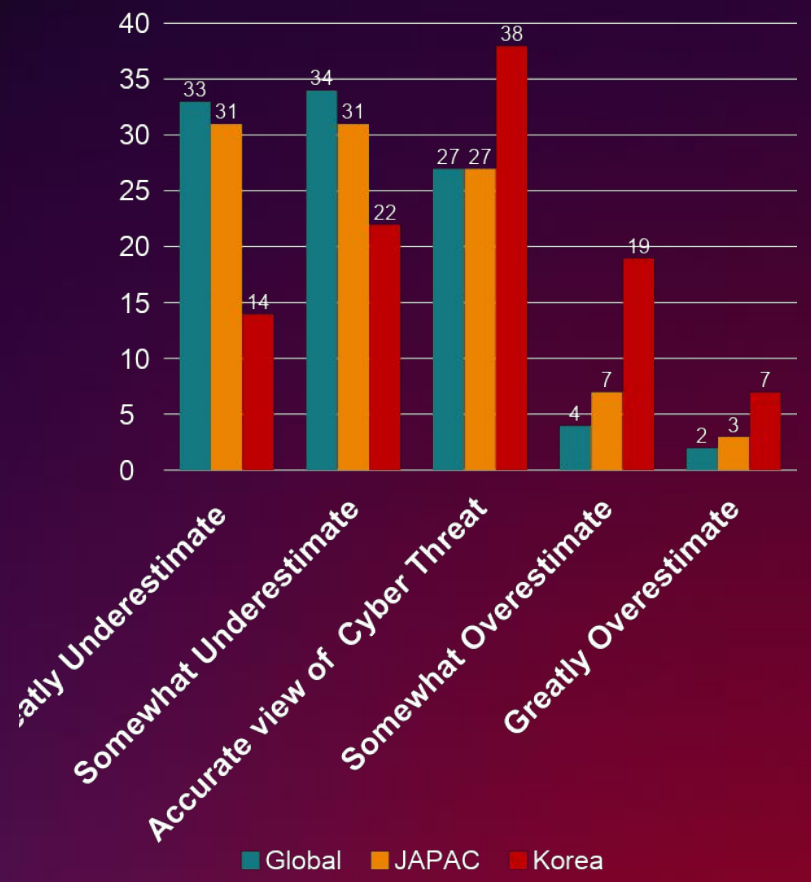
우리 조직의 시니어 리더쉽 및 경영진은 조직의 사이버 위협에 대해 **과소평가** 하고 있다. (Underestimate)

잘 모르고 있고 관심이 별로 없다

27 %(Global)
27 %(JAPAC)
38 %(Korea)

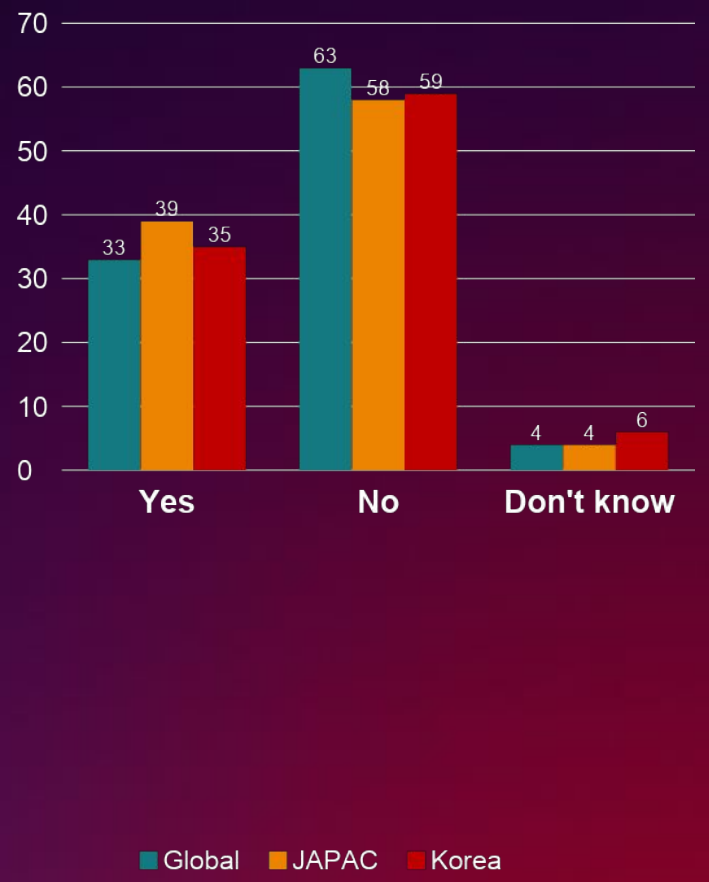
우리 조직의 시니어 리더쉽 및 경영진은 조직의 사이버 위협에 대해 **정확하게 평가** 하고 있다. (Accurate View)

정확하게 판단하고 소홀하게 생각하지 않음



Q2. 지난 12개월 동안 중대한 사이버 공격의 피해를 경험하신 적이 있습니까?

33 %(Global) 39 %(JAPAC) 35 %(Korea)	경험이 있습니다.
63 %(Global) 58 %(JAPAC) 59 %(Korea)	경험이 없습니다.
4 %(Global) 4 %(JAPAC) 6 %(Korea)	모르겠습니다.



Q3. 어떤 종류의 사이버 공격이 당신의 밤잠을 방해할 것 같습니까?
어떤 종류의 공격이 대응에 어려움이 있을 것 같습니까?

Global

1. Ransomware
2. Phishing
3. Malware
4. **Supply Chain**
5. **DDoS**
6. Password Spoof
7. **MITM attack**
8. State-Sponsored
9. Zeroday Exploit

JAPAC

1. Malware
2. Phishing
3. **Supply Chain**
4. Ransomware
5. **MITM attack**
6. **DDoS**
7. Insider attack
8. Password Spoof
9. State-Sponsored

KOREA

1. **MITM attack**
2. **Supply Chain**
3. **DDoS**
4. **Phishing**
5. **State-Sponsored**
6. **Zeroday Exploit**
7. **Password Spoof**
8. **Ransomware**
9. **Insider attack**

Q4. 사이버 보안이 잘 이루어지고 있고 성공적이라고 평가할 수 있는 지표는 무엇입니까?

Global

1. 보안사고 수의 감소 - Reduction in the number of security Incident
2. 침입시도 차단 회수 - The number of intrusion attempts blocked
3. 타사 사이버 보안 평가 결과 - Result of third-party cyber security assessment

JAPAC

1. 침입시도 차단 회수 - The number of intrusion attempts blocked
2. 보안사고 수의 감소 - Reduction in the number of security Incident
3. 타사 사이버 보안 평가 결과 - Result of third-party cyber security assessment

KOREA

1. **적용된 사이버 보안 도구 수 - Number of cyber security tools implemented**
2. **위협평가 및 취약성 검토 - Assessing the threat and reviewing vulns on that basis**
3. **타사 사이버 보안 평가 결과 - Result of third-party cyber security assessment**

- Reduction in the number of security incidents
- The number of intrusion attempts blocked
- Results of third-party cyber security assessments
- Assessing the threat and reviewing vulnerabilities on that basis
- Number of cyber security tools implemented
- **Patching known vulnerabilities**
- The number of security alerts sent out
- **Meeting compliance standards**
- Number of alerts responded to
- Actionable intelligence gained
- Other
- My organization does not measure success when it comes to cyber security
- Don't know

Q5. 조직은 어떤 출처의 정보를 사용하여 위협 상황을 최신으로 유지하고 있습니까? (중복 선택)

ISACs or 유사한 정보공유 그룹 / 내부 위협정보 팀 / 위협정보 제공 전문기업 / 정부기관 프로그램 및 성명서 / 내부 위협 정보 헌터 / 소셜미디어 / 미디어 헤드라인
/ 보안벤더 블로그 / 특별한 소스로부터 정보를 유지 하지 않음

56 %(Global)	ISACs(비영리 위협정보 공유 그룹)
54 %(Global)	조직 내부 자체 위협 인텔 팀
44 %(Global)	위협 인텔리전스 제공자
39 %(Global)	정부 기관의 성명서
38 %(Global)	자체 위협 정보 수집가
37 %(Global)	소셜 미디어
35 %(Global)	미디어 헤드라인
35 %(Global)	보안벤더 블로그

1. 정부기관 및 관련 기관의 정보 공유 (기관의 공식 성명서, 공유정보, 오픈포털 및 비정기 리포트 등)

2. 조직 내부 팀 및 전문인력의 정보 수집 (내부팀의 정보 수집 경로?)

3. 위협인텔리전스 서비스(유/무료)

4. 소셜 / 보안관련 기사 / 블로그 활용

위협정보에 대한 정의와 인지가 부족하고
정확하게 정보의 출처가 어떻게 되는지 알고 있지 못함

소셜/미디어/블로그/기관 정보 등은 일부 예측정보 등이 있을 수 있으나 대부분 사건 사고 소식의 사후 정보

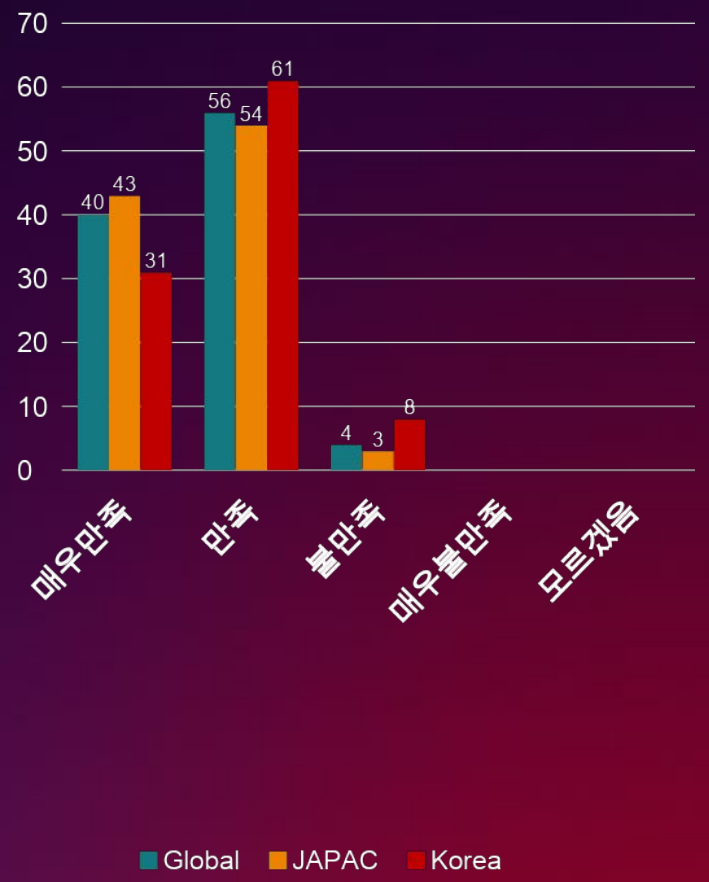
Q6. 조직이 사용하는 위협 인텔리전스의 품질에 얼마나 만족하시나요?

96 %(Global)
97 %(JAPAC)
92 %(Korea)

매우 만족 또는 만족합니다.

4 %(Global)
3 %(JAPAC)
8 %(Korea)

매우 불만족 또는 불만족 합니다.



Q7. 귀사의 조직에는 위협 인텔리전스를 전담하는 직원이 얼마나 있습니까?

	Global	JAPAC	KOREA
1-4 명	2%	2%	2%
5-8 명	9%	8%	4%
9-12 명	26%	**28%**	24%
13-16 명	**28%**	27%	26%
17-20 명	22%	22%	**28%**
21 이상	13%	14%	16%
전담 인원이 없음	1%	0%	0%

위협 인텔리전스 정기적 소스 부족
위협에 대해 과소 평가

위협 인텔리전스 전담 인원이 많다?

아마도
- 위협인텔리전스 전담인원과
  보안관련 업무 인력/조직의 혼동
- 정확한 업무분장의 이해가 부족한
리더쉽의
  가능성도 있음

Q8. 조직이 사용하는 위협 인텔리전스와 관련하여 가장 큰 문제는 무엇입니까?

	Global	JAPAC	KOREA
인텔 정보를 효과적으로 보안 조직에 적용하는 방법	**47%**	**50%**	55%
다른 보안 도구/통제기술과의 통합	40%	42%	53%
보유한 정보로 해야할 것 확인	38%	40%	45%
경보의 적시성	37%	40%	39%
끊임없이 진화하는 위협	**42%**	**43%**	38%
인재 부족/적절한 전문 지식 보유	**43%**	**45%**	37%
변화의 방법	34%	35%	36%
너무 많은 보안 이벤트 경보	33%	34%	34%
보안 관련 예산	25%	20%	20%

Q9. 어떤 공격그룹, 집단 또는 개인이 귀사를 목표로 정했는지를 이해하는 것이 왜 중요하다고 생각하십니까?

	Global	JAPAC	KOREA
사후 대응적인 사이버 보안에서 사전 예방적인 사이버 보안으로 전환	**55%**	54%	**65%**
이해 관계자에게 리스크에 대한 명확한 아이디어 제공	50%	52%	52%
조직을 더 잘 보호하기 위한 조치를 취할 수 있는 능력	**55%**	**59%**	49%
향후 공격에 대한 대비 강화	**56%**	**55%**	43%
동기를 더 잘 이해하기 위해	46%	47%	43%
사이버 공격의 영향 최소화	51%	52%	42%

- 사후 대응적인 사이버 보안에서 사전 예방적인 사이버 보안으로 전환 (KOREA)
- 조직을 더 잘 보호하기 위한 조치를 취할 수 있는 능력 (JAPAC)
- **향후 공격에 대한 대비 강화 (Global)**

Q10. 조직의 사이버 보안에 관련된 결정에 있어서 조직을 목표로 하는 사이버 위협에 대한 이해와 논의 없이 얼마나 자주 이루어집니까? (위협정보와 관계 없이 보안관련 의사 결정이 얼마나 이루어집니까?)

	Global	JAPAC	KOREA
All of the time	25%	24%	20%
The majority of the time	**54%**	**55%**	**59%**
Around half of the time	17%	17%	20%
Rarely	**3%**	**3%**	**1%**
Never	**1%**	**1%**	**0%**

언제나 항상 고려 안함
+
대부분의 경우 고려 안함

Global 69%
JAPAC 79%
KOREA **79%**

Q11. 조직을 목표로 하는 공격 그룹의 전술, 기술 및 절차 (TTP)에 대한 조직은 완벽하게(Comprehensive) 이해하고 있습니까?

35% Global

34% JAPAC

20% KOREA

Q12. 얼마나 자주 조직의 사이버 보안 방어/운영에 대한 진단과 테스트를 진행하십니까?

	Global	JAPAC	KOREA
매일 점검	14%	11%	7%
주간 점검	**32%**	**32%**	21%
격주 점검	23%	26%	**39%**
월간 점검	19%	22%	23%
분기 점검	8%	7%	9%
반기 점검	2%	1%	0%
년간 점검 또는 그보다 적게	1%	1%	1%

Q13. 사이버 공격 또는 침해가 발생했을 경우 어떤 국가의 지원을 받은 공격그룹이 가장 방어/대응하기 힘든 국가일까요?

Global

22%

RUSSIA

20%

CHINA

15%

NORTH KOREA

12%

IRA

30%

Can Fully Defense

JAPAC

22%

CHINA

21%

RUSSIA

16%

NORTH KOREA

13%

IRA

27%

Can Fully Defense

KOREA

22%

NORTH KOREA

21%

CHINA

17%

RUSSIA

17%

IRA

23%

Can Fully Defense

Q14. 아래의 가정에 어느정도 동의/비동의 하십니까?

“조직이 가지고 있는 수준 높은 위협 인텔리전스는 더 개선 될 수 있다(부족한 부분이 있다)”

66%(Global) 66%(JAPAC) 85%(Korea)

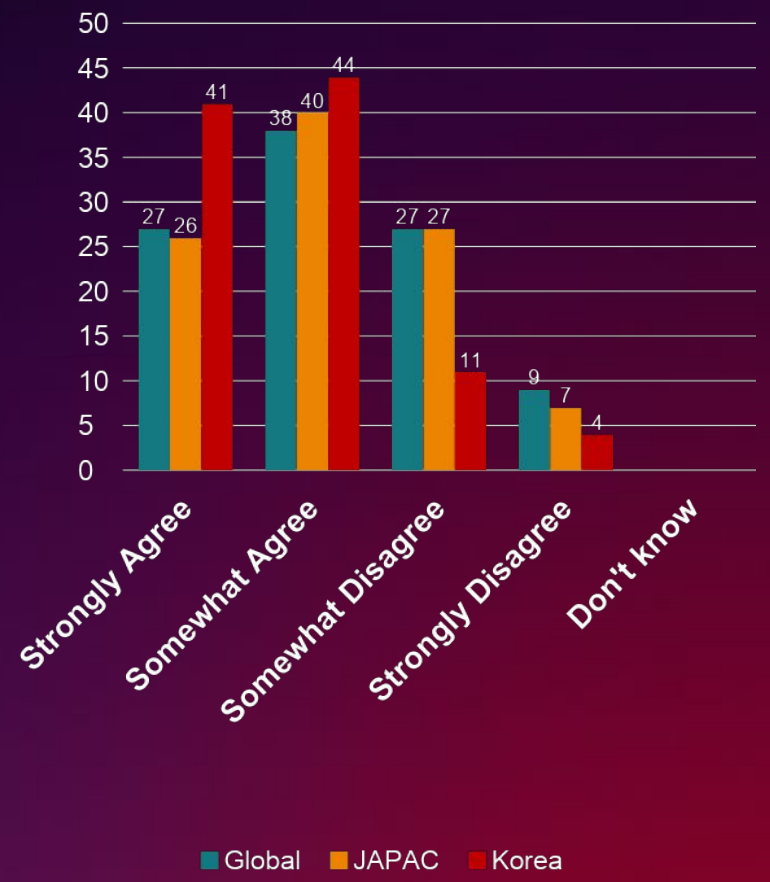
매우 동의하거나
어느정도 동의 합니다.

네, 위협인텔리전스는 개선되어야 합니다.

35 %(Global)
34 %(JAPAC)
15 %(Korea)

매우 동의하지 않거나
어느정도 동의 하지 않습니다.

아니요, 위협인텔리전스는 충분 합니다.



Q15. 아래의 가정에 어느정도 동의/비동의 하십니까?

"너무 많은 위협 인텔리전스 정보를 가지고 있어서 이에 대해 모든 조치를 취할 수가 없다"

41%(Global) 39%(JAPAC) 45%(Korea)

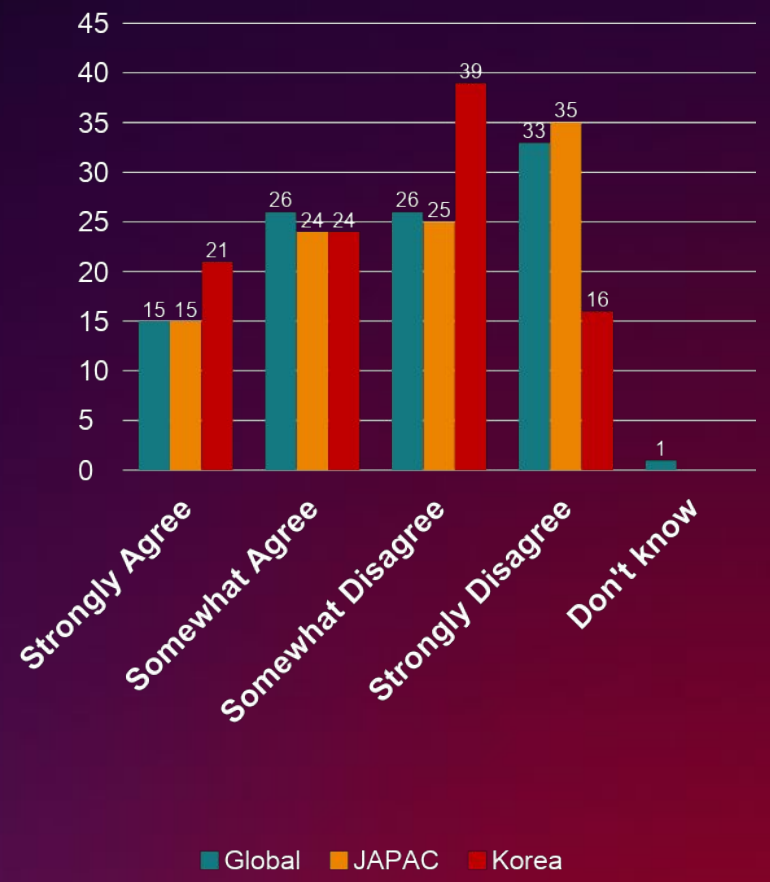
매우 동의하거나
어느정도 동의 합니다.

네, 정보가 너무 많아서 대응이 어렵습니다.

59 %(Global)
60 %(JAPAC)
55 %(Korea)

매우 동의하지 않거나
어느정도 동의 하지 않습니다.

아니요, 정보가 너무 많아도 대응이 가능합니다.



Q16. 아래의 가정에 어느정도 동의/비동의 하십니까?

“사이버 보안 인력 부족으로 인해 조직이 최신 위협에 대처할 수 없습니다”

53%(Global) 52%(JAPAC) 68%(Korea)

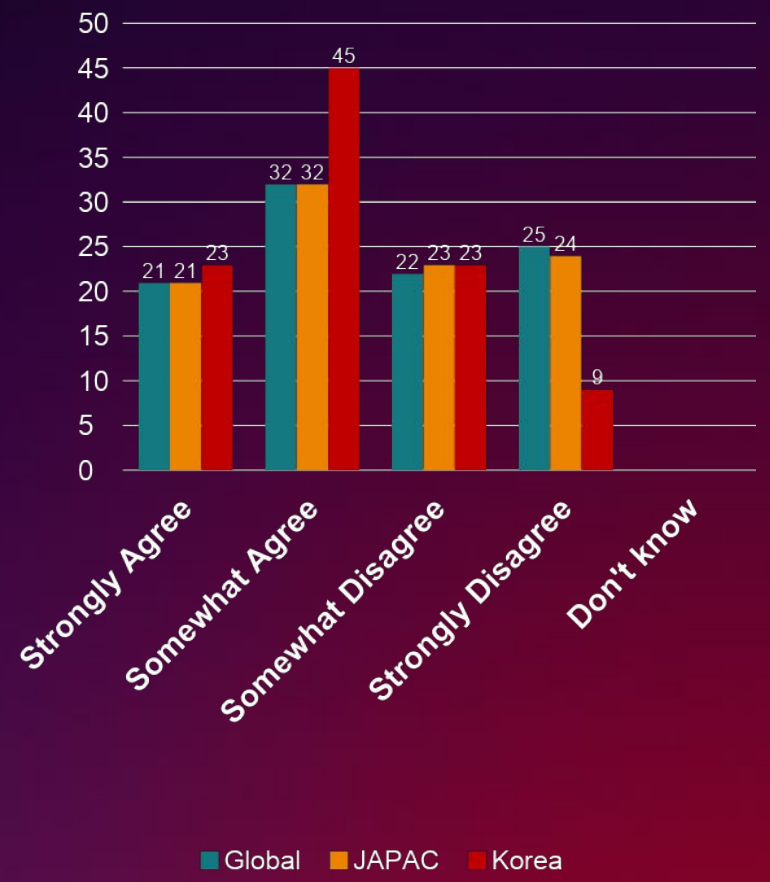
매우 동의하거나
어느정도 동의 합니다.

네, 인력이 부족합니다.

47 %(Global) 47 %(JAPAC) 32 %(Korea)

매우 동의하지 않거나
어느정도 동의 하지 않습니다.

아니요, 인력은 부족하지 않습니다.

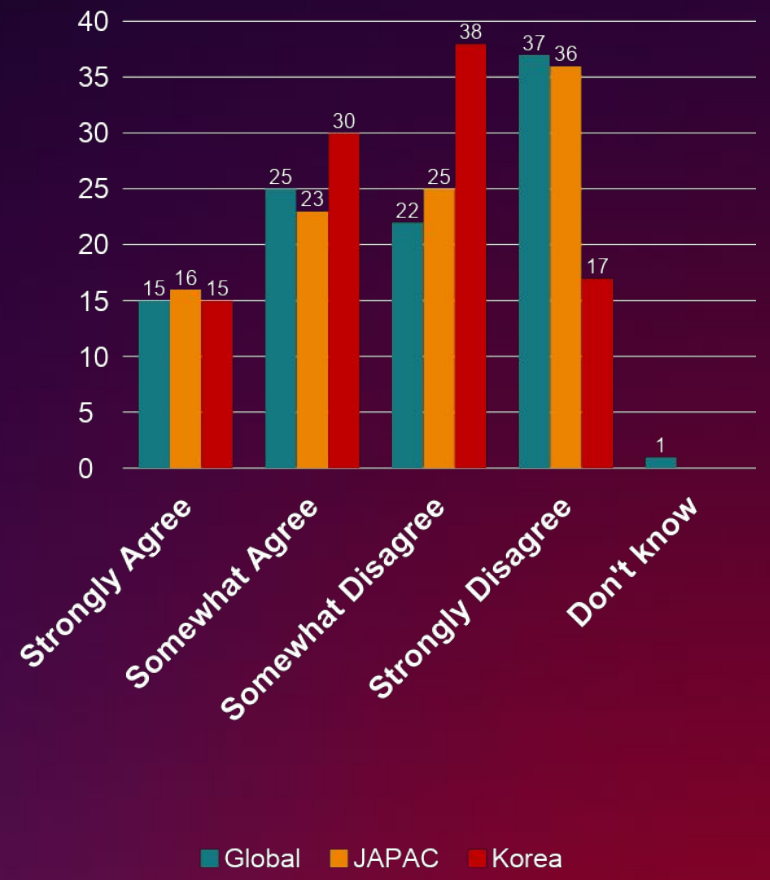


Q17. 아래의 가정에 어느정도 동의/비동의 하십니까?

"조직이 최신 사이버 위협을 대처하기 위한 보안 팀의 예산이 충분하지 않습니다."

40 %(Global)	매우 동의하거나
39 %(JAPAC)	어느정도 동의 합니다.
45 %(Korea)	네, 충분하지 않습니다.

59 %(Global)	매우 동의하지 않거나
61 %(JAPAC)	어느정도 동의 하지 않습니다.
55 %(Korea)	아니요, 충분합니다.



MANDIANT
NOW PART OF Google Cloud

Some Findings

조직은 아래 공격그룹에 대한 준비가 되어
있습니다. (KOREA)

83%
Financially Motivated Actor

90%
Hacktivist Actor

94%
Nation-State Actor

국가 공격이 발생할 경우 다음 중 귀사가 완전히 방어할 수 없는 국가는 어디라고 생각하십니까?

	Russia	China	N.Korea	Iran
KOREA	55%	61%	54%	61%
JAPAC	58%	54%	67%	47%
Global	57%	53%	52%	44%

68% (Global)
의 응답자는 조직이 전반적인 위협에 대한 이해도를 개선해야 한다고 생각합니다.

71% (JAPAC)
의 응답자는 조직이 전반적인 위협에 대한 이해도를 개선해야 한다고 생각합니다.

87% (KOREA)
의 응답자는 조직이 전반적인 위협에 대한 이해도를 개선해야 한다고 생각합니다.

MANDIANT
NOW PART OF Google Cloud

Some Findings (Global)

96% 의 응답자는 조직이 사용하고 있는 위협 인텔리전스의 품질에 만족

96% 의 응답자는 보안 의사 결정자들은 어떤 사이버 위협 행위자들이 그들의 조직을 목표로 할 수 있는지 이해하는 것이 중요하다고 믿음

79% 의 응답자는 사이버위협에 대한 전반적인 이해 및 검토 없이 중요한 결정이 매우 많이 이루어진다고 응답

67% 의 응답자는 조직의 고위 경영진 및 결정권자들이 사이버 위협을 과소평가(중요하지 않게) 하고 있다고 응답

47% 의 응답자는 보안을 담당하는 조직 전체에 위협 인텔리전스를 효과적으로 적용하는 것이 가장 큰 과제라고 응답

"THREAT INTELLIGENCE IS IMPORTANT BUT IT'S NOT RELATED WITH YOUR BUSINESS"

WHY?!

MANDIANT
NOW PART OF Google Cloud

사이버 위협 인텔리전스를 효과적으로 운영하고 투자 가치를 극대화하려면

Evaluate the data you rely on to ensure it is trustworthy, timely and actionable

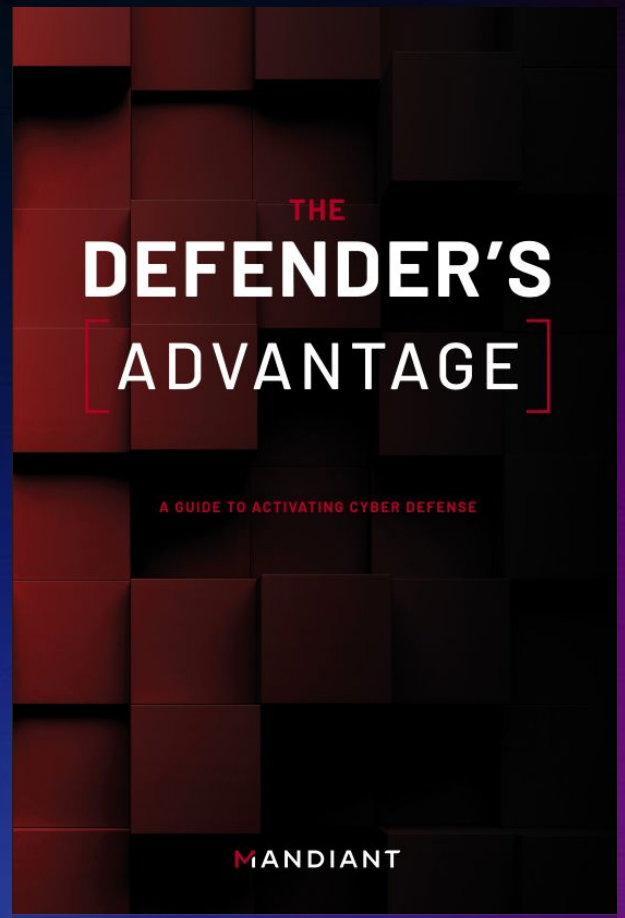
Understand active threats specific to your organization and industry

Communicate with your stakeholders

Prioritize resources to address what really matters

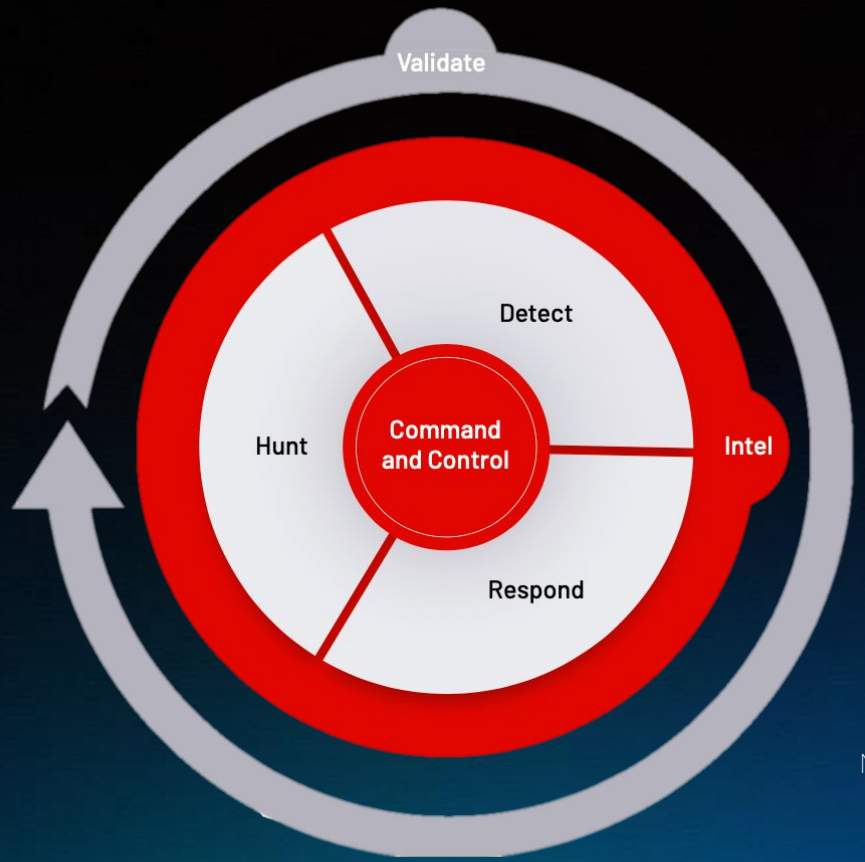
Test your defenses

Take Action



MANDIANT
NOW PART OF Google Cloud

사이버 위협 인텔리전스를 효과적으로 운영하고 투자 가치를 극대화하려면



Intelligence
Guiding Light

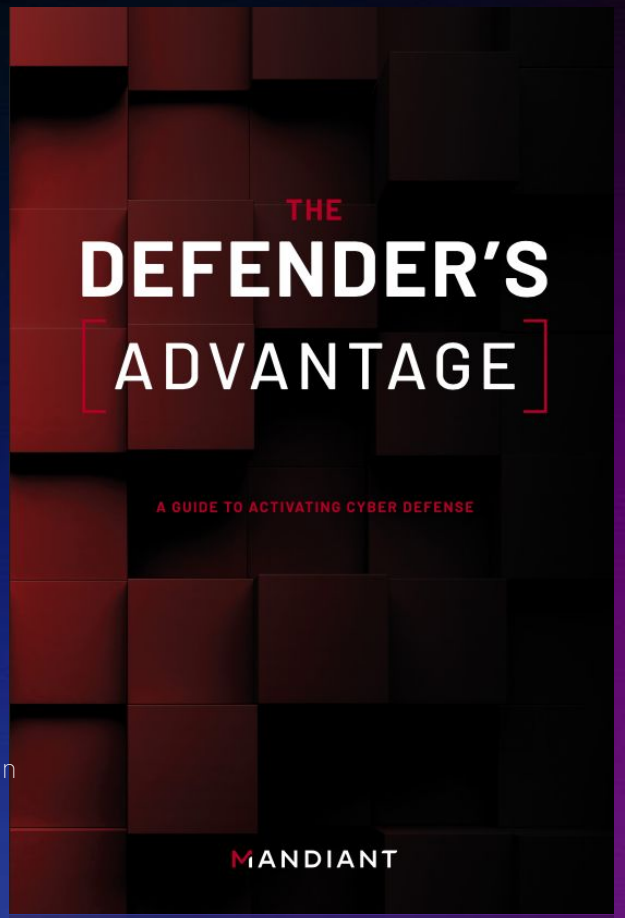
Hunt
Threat Hunting and Compromise Assessment

Respond
Incident Response And Recovery

Command and Control
Maintain the Mission

Detect
Alert Monitoring And Investigation

Validate
Targeted Testing And Controls Validation



MANDIANT
NOW PART OF Google Cloud

Global No.1 Mandiant

Threat Ready with Mandiant

MANDIANT
NOW PART OF Google Cloud

Thank You