quaxar

Leveling up your Cyber Threat Intelligence

CTI 필요성 및 기업 내 CTI 조직 활용방안

김재기 팀장 / CTI(TALON) Division

What?

사이버 위협 인텔리전스 (CTI)

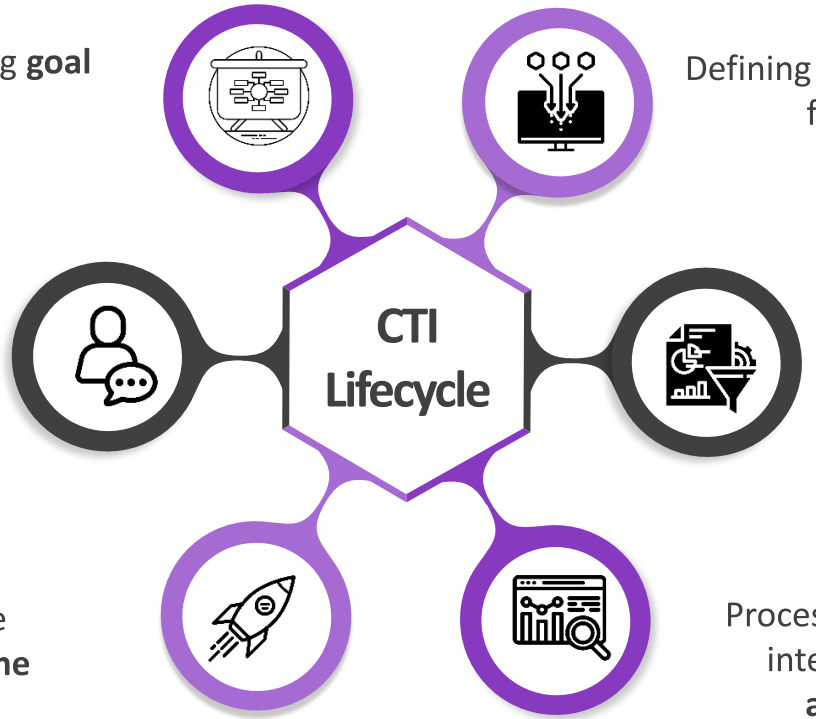
Intelligence != Information

1. 계획

Defining a CTI **mission** & setting **goal**
Identifying the attack surface
and the most valuable **assets**

2. 수집

Defining **what** should be collected to
fulfill requirements/planning



3. 처리

Data is stored, sanitized,
and converted into
a **meaningful information**

4. 분석

Processed information is **analyzed**,
interpreted , and converted into
actionable threat intelligence

5. 전달

Delivering **finished** intelligence
to stakeholders at the **right time**

6. 피드백

Stakeholders **reviewing** the
final intelligence product and
make a comment based on
their planning phase

사이버 위협 인텔리전스 (CTI)

Intelligence with Stakeholders

1. 계획

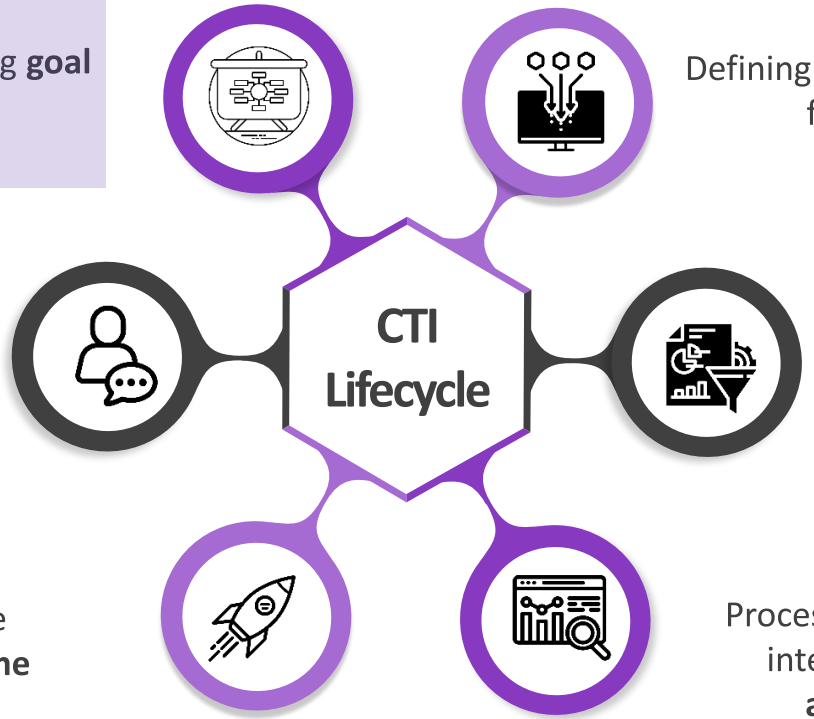
Defining a CTI **mission** & setting **goal**
Identifying the attack surface
and the most valuable **assets**

6. 피드백

Stakeholders **reviewing** the
final intelligence product and
make a comment based on
their planning phase

5. 전달

Delivering **finished** intelligence
to stakeholders at the **right time**



2. 수집

Defining **what** should be collected to
fulfill requirements/planning

3. 처리

Data is stored, sanitized,
and converted into
a **meaningful information**

4. 분석

Processed information is **analyzed**,
interpreted , and converted into
actionable threat intelligence

S2W

Why?

사이버 위협 인텔리전스
???? 보안 서비스

사이버 위협 인텔리전스 서비스

기반

주도

중심

사이버 위협 인텔리전스 제공 보안 서비스

> The role of intelligence is to **inform the decision-making process**, **support the policies**, and provide **knowledge** and **decision advantages** for the policy maker
> (Amanda J. Gookins)

S2W

사이버 위협 인텔리전스 서비스

사이버 위협 인텔리전스 제공 보안 서비스

→ 구독 서비스와 유사

사이버 위협 인텔리전스 서비스

사이버 위협 인텔리전스 제공 보안 서비스

→ 구독 서비스 : **컨텐츠**가 중요

사이버 위협 인텔리전스 서비스

사이버 위협 인텔리전스 컨텐츠가 중요

Malware

Vulnerability

Incidents

Data Breach

Threat Actor

Abusing

사이버 위협 인텔리전스 서비스의 필요성

사이버 위협 인텔리전스 컨텐츠

Malware	랜섬웨어, 스틸러, 봇넷, 백도어, 원격제어형 …
Vulnerability	각종 취약점 정보 (Spring4shell, Log4shell, Dirty-Pipe, Proxyshell) …
Incidents	LAPSUS$, Gwisin, BGP 하이재킹, 월패드 이슈 …
Data Breach	딥웹 포럼, 다크웹 기반 유출 사이트, 소셜 미디어, 텔레그램, 표면웹 상에 노출된 민감 정보 …
Threat Actor	국가 배후 공격 그룹, 사이버 범죄 조직, 딥/다크웹 포럼 사용자 …
Abusing	유사 도메인, 정상 서비스/명령어를 악용한 공격(Living-Off-the-Land Attacks) …

사이버 위협 인텔리전스 서비스의 필요성

사이버 위협 인텔리전스 컨텐츠 : S2W Original & Exclusive

Malware	랜섬웨어, 스틸러, 봇넷, 백도어, 원격제어형 …
Vulnerability	각종 취약점 정보 (Spring4shell, Log4shell, Dirty-Pipe, Proxyshell) …
Incidents	LAPSUS$, Gwisin, BGP 하이재킹, 월패드 이슈 …
Data Breach	딥웹 포럼, 다크웹 기반 유출 사이트, 소셜 미디어, 텔레그램, 표면웹 상에 노출된 민감 정보 …
Threat Actor	국가 배후 공격 그룹, 사이버 범죄 조직, 딥/다크웹 포럼 사용자 …
Abusing	유사 도메인, 정상 서비스/명령어를 악용한 공격(Living-Off-the-Land Attacks) …
S2W	**TALON REPORT** (악성코드, 취약점, 위협그룹, 민감정보 유출 및 내부 자산 노출 정보 …), **Professional Service** (침해사고 조사, 악의적인 컨텐츠에 대한 차단 [Take-Down] …), **S2Gehter** (커뮤니티), **Active Intelligence** (주요 악성코드 및 위협그룹 추적/조사, 연관성 분석 및 그래프 제공, 광범위한 채널 커버 …) **Exclusive Intelligence** (유효성이 높은 고객사 맞춤형 위협 정보 – 평균 80% 이상)

사이버 위협 인텔리전스 서비스의 필요성

사이버 위협 인텔리전스 컨텐츠 : S2W Original & Exclusive

- Malware
- Vulnerability
- Incidents
- Data Breach
- Threat Actor
- Abusing
- S2W

(합리적인 의사 결정 지원) 다양한 사이버 위협에 대한 예측, 준비, 예방, 대응

(리더쉽 지원) 기존 또는 신규 위협에 대한 전략적,전술적, 운영적 결정

(비지니스 리스크 식별 및 완화) 알려지지 않은 위협을 알려진 위협으로 전환

(기존 보안 강화) 공격자에 대한 TTP 식별, 다양한 위협에 대한 통합 활용

How?

기업 내 사이버 위협 인텔리전스 조직 활용방안

기업 내 사이버 위협 인텔리전스 활용을 위한 준비

1) **보안사고 관리** 프로세스 확립

2) **코어 SOC 기술** 확립 (예: SIEM, EDR, IDS, IPS ...)

3) 확립된 정책 및 기술은 **자동화** 된 **위협 정보**를 수신 및 적용 할 수 있어야 함
(예: IoC, YARA Rules, Credentials, Attack Surface Monitoring ...)

When?
&
Who?

사이버 위협 인텔리전스 서비스의 필요성

사이버 위협 인텔리전스 컨텐츠

- Malware
- Vulnerability
- Incidents
- Data Breach
- Threat Actor
- Abusing
- S2W

(합리적인 의사 결정 지원) 다양한 사이버 위협에 대한 예측, 준비, 예방, 대응

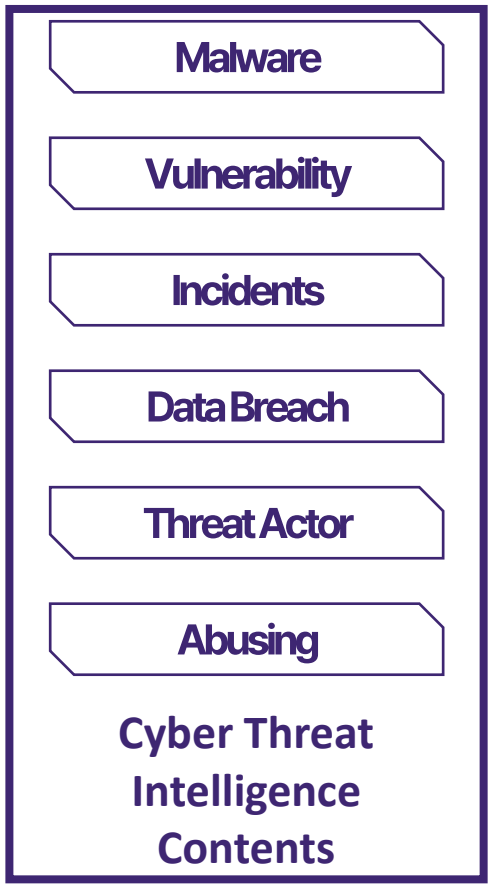
(리더쉽 지원) 기존 또는 신규 위협에 대한 전략적,전술적, 운영적 결정

(비지니스 리스크 식별 및 완화) 알려지지 않은 위협을 알려진 위협으로 전환

(기존 보안 강화) 공격자에 대한 TTP 식별, 다양한 위협에 대한 통합 활용

기업 내 사이버 위협 인텔리전스 조직 활용방안

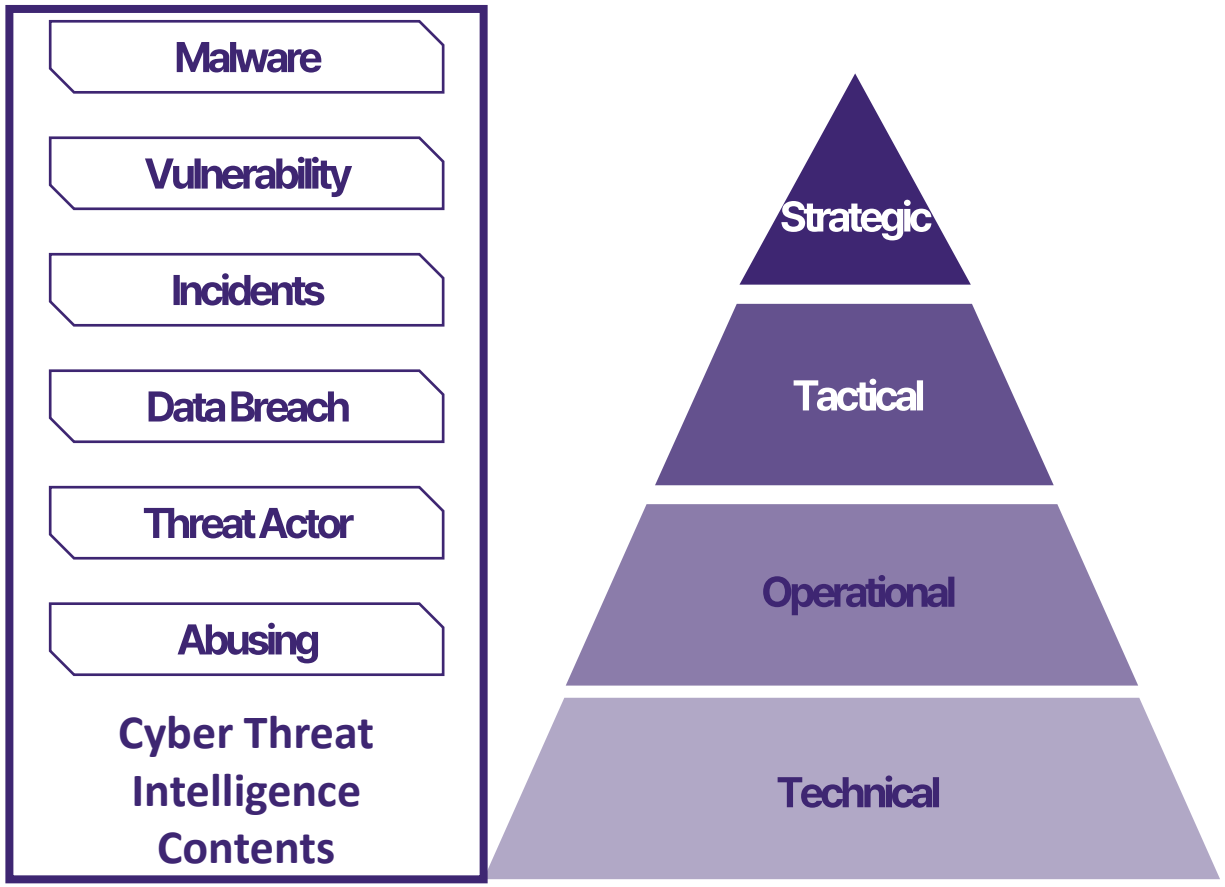
사이버 위협 인텔리전스 컨텐츠



S2W

기업 내 사이버 위협 인텔리전스 조직 활용방안

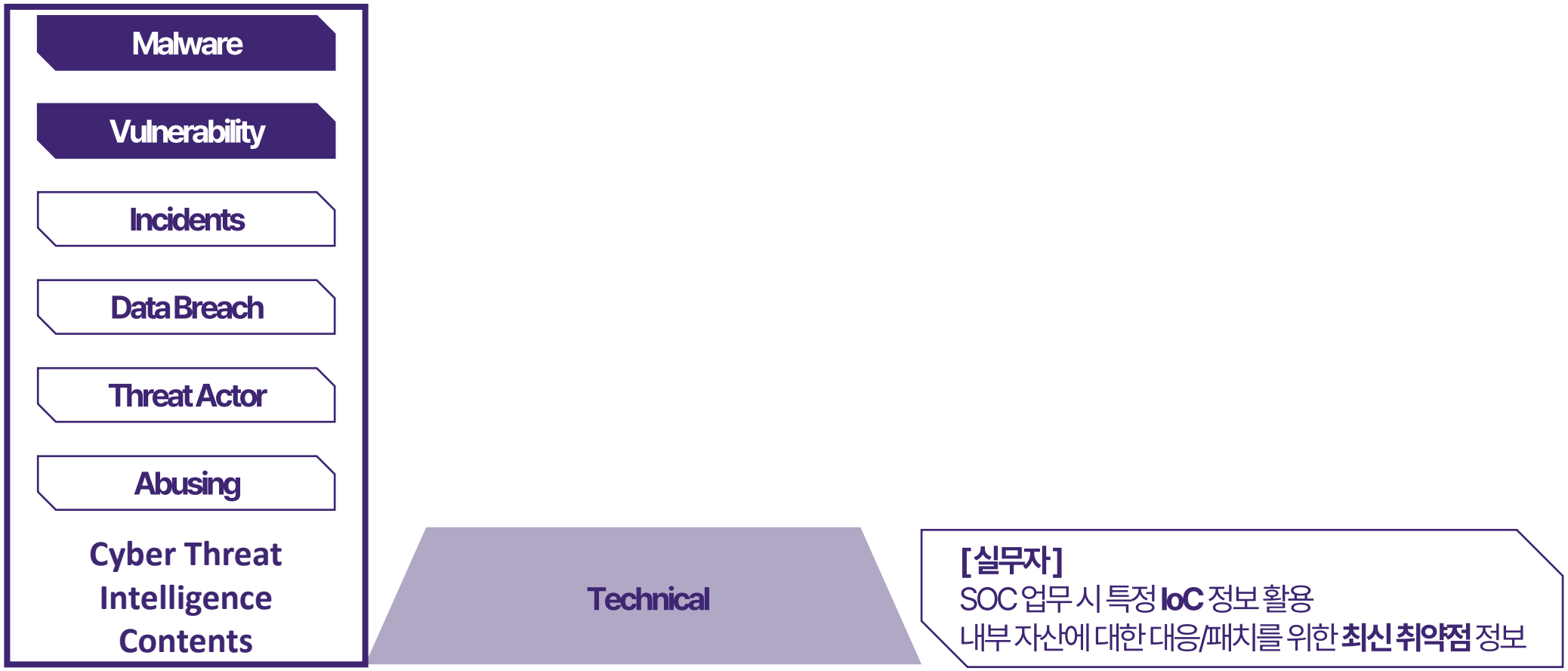
기업 내 역할별 사이버 위협 인텔리전스 활용방안 - 일반 상황



S2W

기업 내 사이버 위협 인텔리전스 조직 활용방안

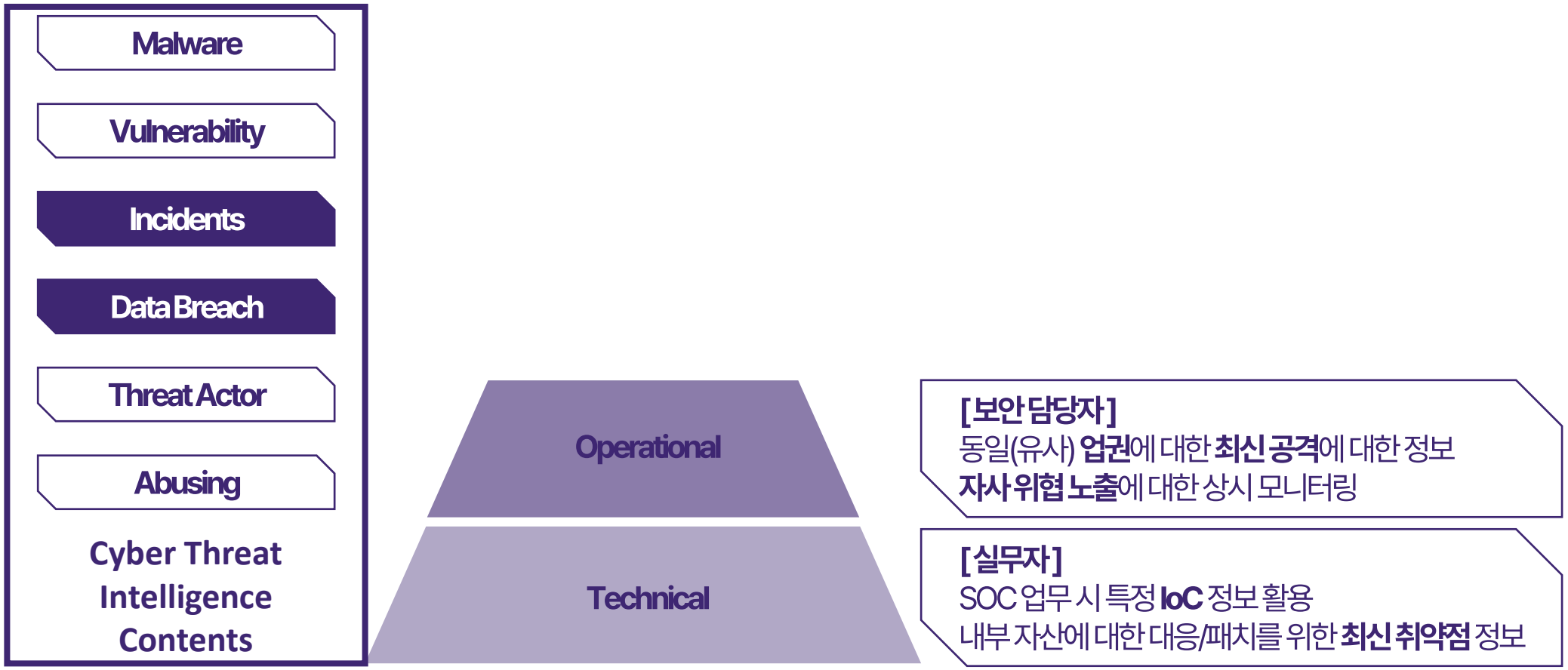
기업 내 역할별 사이버 위협 인텔리전스 활용방안 - 일반 상황



S2W

기업 내 사이버 위협 인텔리전스 조직 활용방안

기업 내 역할별 사이버 위협 인텔리전스 활용방안 - 일반 상황



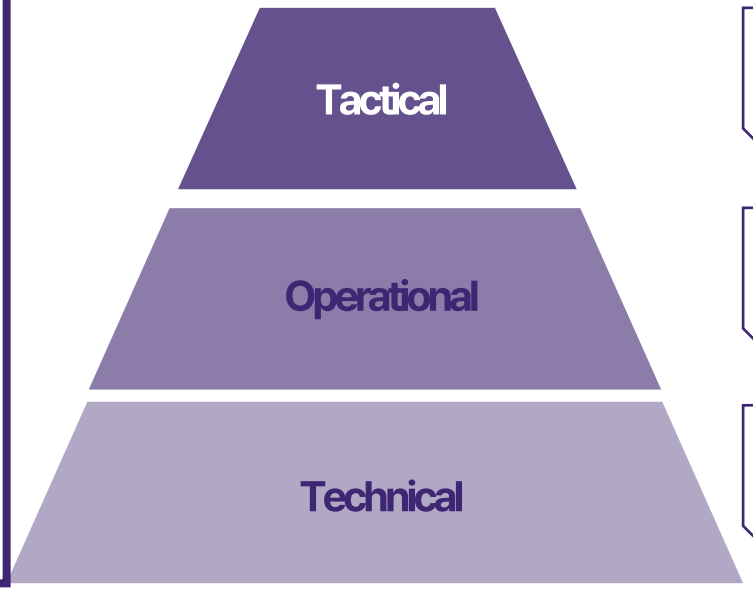
S2W

기업 내 사이버 위협 인텔리전스 조직 활용방안

기업 내 역할별 사이버 위협 인텔리전스 활용방안 - 일반 상황

- Malware
- Vulnerability
- **Incidents**
- Data Breach
- **Threat Actor**
- Abusing

Cyber Threat Intelligence Contents



[관리자]
동일(유사) **업권 침해사고**의 **시사점**
및 식별된 **공격자**에 대한 **TTP** 정보

[보안 담당자]
동일(유사) **업권**에 대한 **최신 공격**에 대한 정보
자사 위협 노출에 대한 상시 모니터링

[실무자]
SOC 업무 시 특정 **IoC** 정보 활용
내부 자산에 대한 대응/패치를 위한 **최신 취약점** 정보

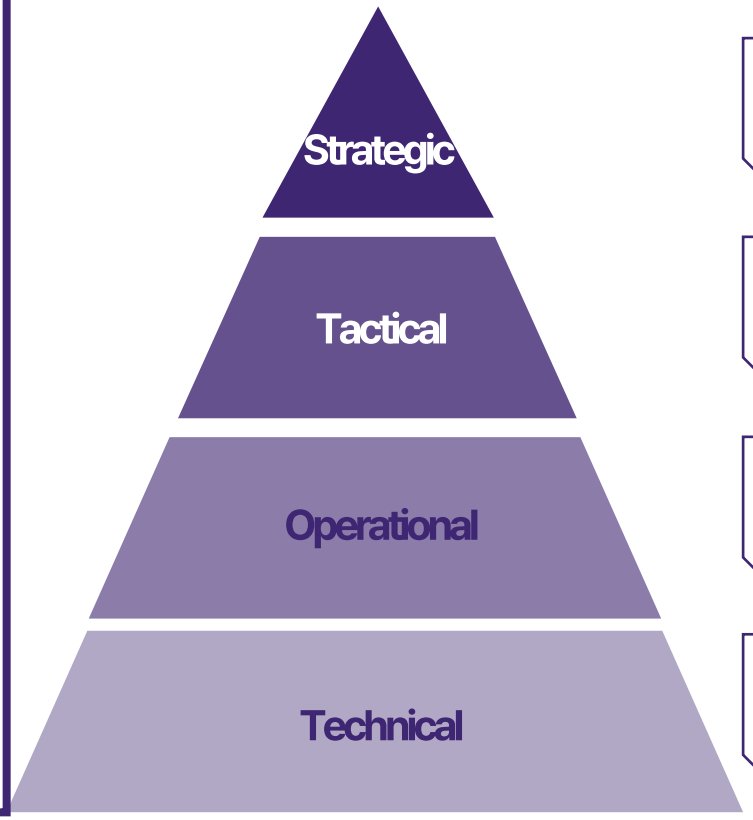
S2W

기업 내 사이버 위협 인텔리전스 조직 활용방안

기업 내 역할별 사이버 위협 인텔리전스 활용방안 - 일반 상황

- Malware
- Vulnerability
- Incidents
- Data Breach
- Threat Actor
- Abusing

Cyber Threat Intelligence Contents



[C-Level]
비지니스 상 **리스크 대응(측정)**에 대한 **의사 결정** 지원

[관리자]
동일(유사) **업권 침해사고**의 **시사점** 및 식별된 **공격자**에 대한 **TTP** 정보

[보안 담당자]
동일(유사) **업권**에 대한 **최신 공격**에 대한 정보
자사 위협 노출에 대한 상시 모니터링

[실무자]
SOC 업무 시 특정 **IoC** 정보 활용
내부 자산에 대한 대응/패치를 위한 **최신 취약점** 정보

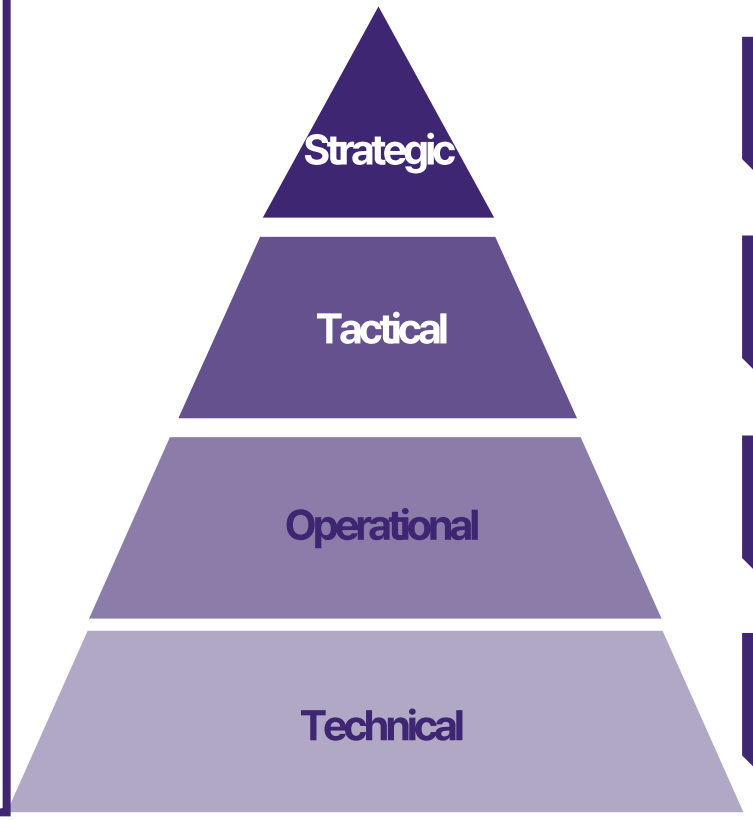
S2W

기업 내 사이버 위협 인텔리전스 조직 활용방안

기업 내 역할별 사이버 위협 인텔리전스 활용방안 - 사고 발생

- Malware
- Vulnerability
- Incidents
- Data Breach
- Threat Actor
- Abusing

Cyber Threat Intelligence Contents



S2W - Exclusive

[C-Level]
침해사고 조사 및 고객 대응을 위한 정확한 상황 파악과 관련 의사 결정

[관리자]
유출 정보의 전파를 막기 위한 모니터링 정책 강화 및 악의적인 컨텐츠 차단 (**Take-Down**) 보고

[보안 담당자]
사고 범위 및 원인 파악을 위한 내부 자산과 밀접한 위협 정보 확인 및 보고 (예: **내부망 접근 계정 정보**)

[실무자]
YARA Rule 등을 활용한 **악성코드 식별**
보안 솔루션 내 로그 데이터 중 일치하는 **IoC** 확인

S2W

Conclusion

결론

For Actionable Intelligence

외부 위협에 대한
내재화

산업군별 특성에
대한 이해도 필요

사소한 것도 공유하자
(feat. Community)

CTI 서비스 제공자와
고객 사이 간극 최소화

S2W

Where?

S2W와 솔루션에 대해 더 알고 싶으신가요?

S2W의 문은 언제나 열려있습니다, 아래의 메일 주소로 문의주세요.

info@s2w.inc

www.s2w.inc
경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277