K-CTI 2020

공격자 보다 먼저 보안 위협 찾기
Threat Hunting

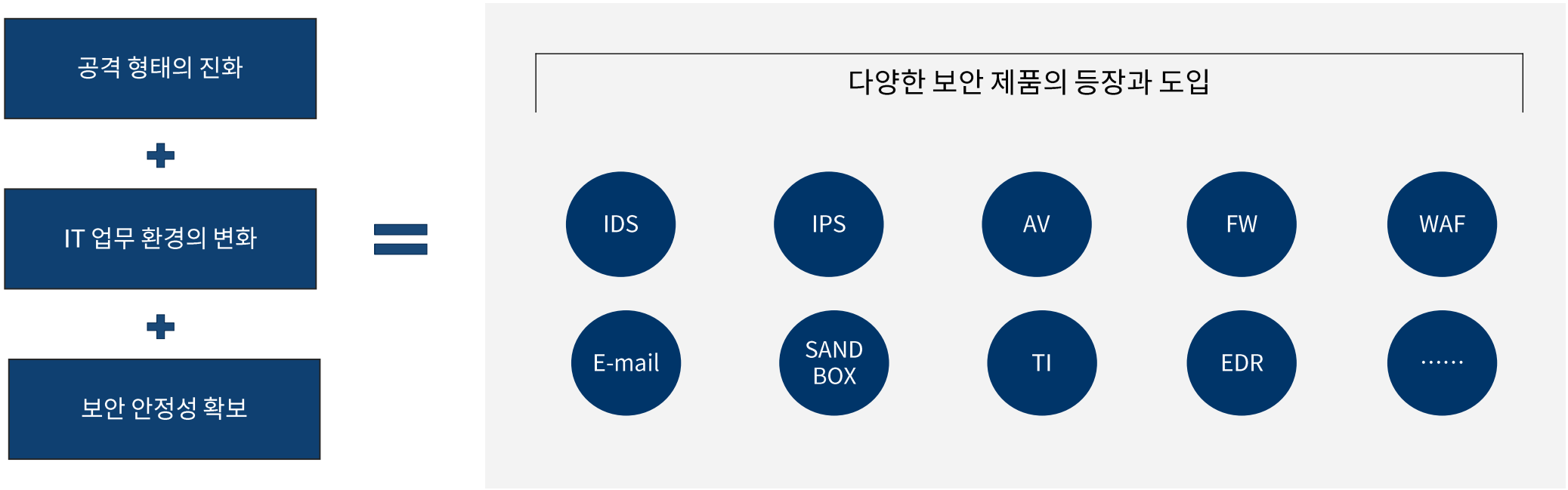
NCSOFT

K-CTI 2020
2020 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

목차

배경

> 고도화 , 지능화 된 공격자의 보안 위협과 기술의 발전으로 IT 업무 환경의 변화 속에서
> 보안 안정성을 확보 하기 위한 많은 노력 !



배경

이벤트는 점점 증가 되고 수많은 이벤트에서 모든 위협을 탐지 할 수 있는가?
모든 구간에 대하여 가시성은 확보 되어 있는가?

1. 방대한 이벤트에서 모든 위협을 잘 탐지 하고 있을까? **‘탐지’**
2. 모든 구간을 빠짐 없이 모니터링 하고 있을까? **‘가시성’**
3. 보안 설정이 미흡 하거나 설정을 우회 하는 위협이 있지 않을까? **‘보안 취약성’**

“ 우리 회사는 보안 위협에 대하여 안전한가? ”

배경

탐지 개선

가시성 확보

보안 설정 강화

기존 보안 구성

수동 적이며 절차를 중시

- 웹 과 서비스 위주의 진단
- 설정 값 확인 위주의 점검
- 자동화된 방어 및 탐지

공격자 입장 관점

능동적이고 추상적임

- 접근 가능 한 모든 접점
- 보안 설정의 우회
- 공격 과정의 흔적 제거

배경

"**Threat Hunting**은 **분석 기반 접근(Analyst-Centric Process)**이며 기존 탐지 또는 차단 시스템이 인지하지 못했던 숨어있는 **고도의 위협을 찾아내는 과정**"

[가트너 애널리스트] - 안톤 슈바킨(Anton Chuvakin)
가트너 시큐리티&리스크 매니지먼트 서밋 2018 발표

" 사고가 발생하기 전에 피해를 예방하거나 피해 최소를 위한 위협을 적극적으로 찾는 것 "

배경

Threat Hunting ??

“용어는 많이 들어 봤지만 어떻게 시작 해야 되는지 모르겠어요.”

해외 위주의 연구 자료

국내 적용 사례 부족

“ 직접 부딪치며 NCSOFT 만의 Threat Hunting 체계를 만들자 ”

NC Threat Hunting

공격자 분석

공격 기법 조사

내부 현황 확인

NC Threat Hunting

사이버 위협 모델

Threat Attack Model 선정하기

체계적인 Threat Hunting을
하기 위해 공격자의 공격 형태를 연구

Lockheed Martin
'Cyber Kill Chain'

FireEye
'Attack Lifecycle'

Gartner
'Cyber Attack Model'

MITRE
'ATT&CK Lifecycle'

사이버 위협 모델

그냥 알려진 모델 중 하나만 선택 해서 사용하면 될까?

기업 보안에서 정말 맞는 모델일까?

우리 엔씨소프트의 환경에 맞을까?

사이버 위협 모델

다양한 침해 사고에 대한 분석 및
공격 형태에 대한 파악이 우선!

- 외부 침해사고 사례 조사
- 내부 공격 히스토리 분석
- APT 공격 그룹 조사
- 공격 유형 조사

사이버 위협 모델

정찰 Recon	• 구글링, 주변 탐색 • 악성코드 제작 또는 취약점 코드제작 • 기업의 인프라 밖에서 진행 됨
무기화 Weaponization	
유포 Delivery	• 기업 인프라 접근 시도 • 취약점 공격 • 악성코드 설치 및 공격 • 자료 유출 • 기업 내에 공격자가 침입하여 활동
악용 Exploitation	
설치 Installation	
명령 및 제어 Command & Control	
목적 달성 Actions on Objectives	

위협 정보를 활용하여 사전 차단

탐지 및 가시성을 확보하고
취약점이 제거 되어 하는 부분

NC Attack Lifecycle

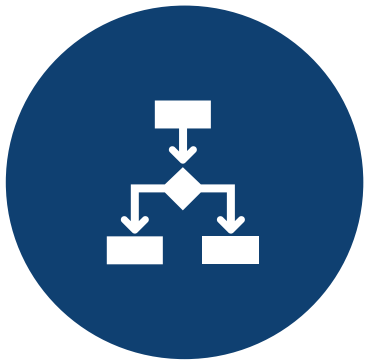
NC Attack Lifecycle

초기 접근

- 사내 인프라에 접근 시도
- 악성코드 전달
- 악성코드 실행 등

장악

- 호스트에 대한 거점 확보를 위한 행위
- 악성코드 은닉/지속
- 보안장비 탐지 우회 등



확산

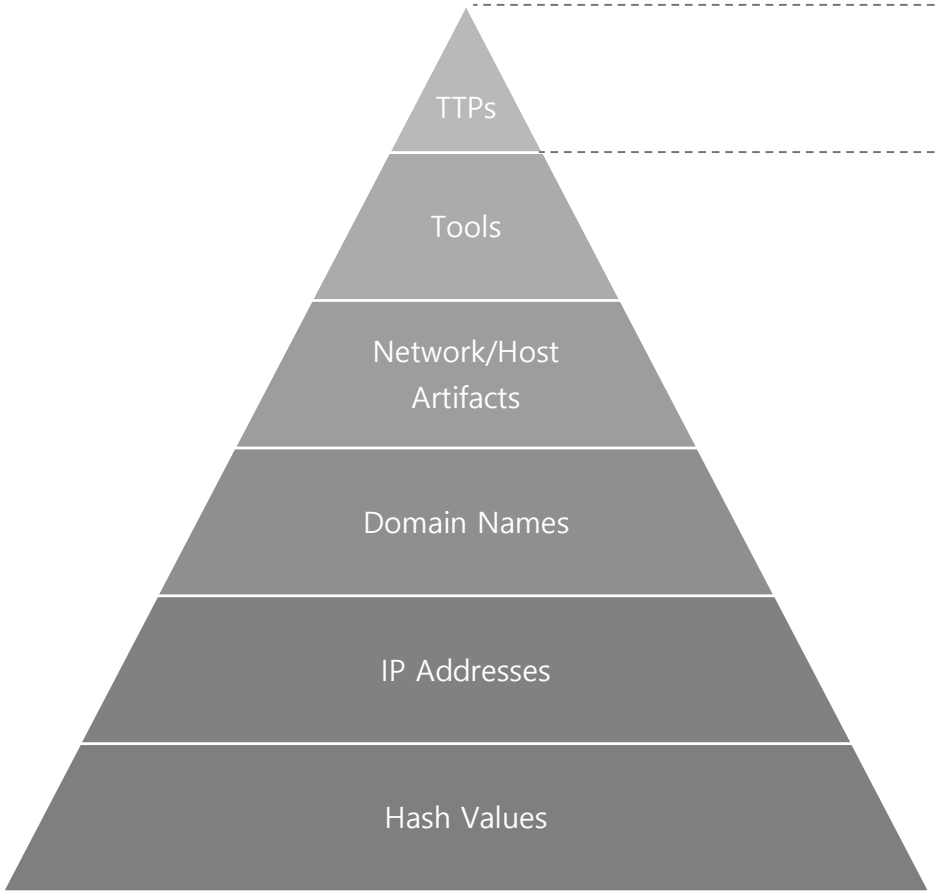
- 주변 호스트로 확산 하기 위한 행위
- 내부정보 수집
- 인증 탈취 등

목적 달성

- 공격자의 목적을 달성 하기 위한 행위
- 시스템 파괴
- 정보 유출 등

Tactics, Techniques and Procedures

공격자는 어떠한 기술로 공격을 할까?



공격자의 전략, 전술 및 절차를 기반으로 한 IOC

공격자는 지속적인 공격을 하기 위하여
Adm1n 이름으로 관리자 계정을 생성 하였다.

패턴 중심의 탐지

- Adm1n 이라는 Value가 탐지 중심
- 계정명이 변화하면 탐지가 어려움

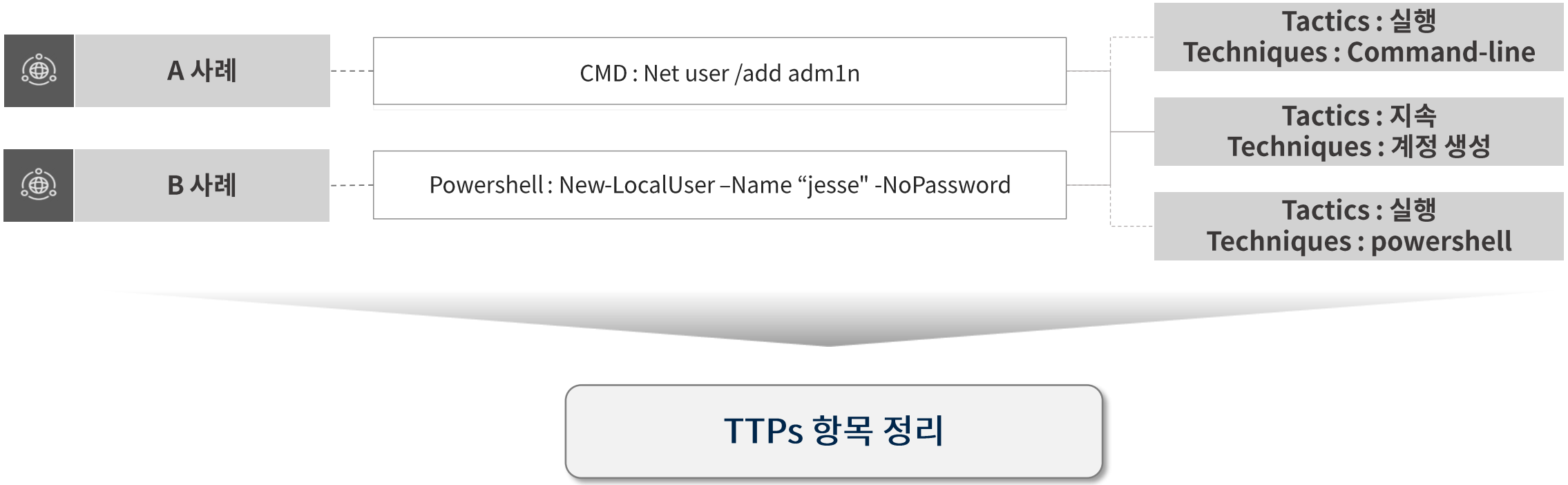
TTPs

- Tactics : 지속
- Techniques : 관리자 계정 생성
- 공격자의 관점으로 의도와 기술을 파악 하여 탐지

Tactics, Techniques and Procedures

TTPs 정리

“ 침해 사고 사례를 TTPs 형태로 목록화”



Tactics, Techniques and Procedures

초기	장악	확산	목적달성
주요 서비스 사용	스케줄러 등록	시스템 정보 수집	내부 데이터 유출
웹 서비스 사용	자동 실행 등록	네트워크 정보 수집	리소스 하이재킹
기타 서비스 사용	서비스 생성	도메인 계정/그룹 수집	데이터 압축
취약점 사용	서비스 실행	로컬 계정/그룹 수집	데이터 변조
웹 취약점 사용	서비스 변조	공유 자원 정보 수집	데이터 삭제
악성메일	서비스 중지	인증 정보 획득	암호화 전송
소프트웨어 업데이트	서비스 삭제	원격 연결 정보 수집	Denial of Service
사용자 브라우저 확장 프로그램 설치	프로그램 파일 변조	서비스 포트 스캔	금전적 피해
사용자 프로그램 설치	시스템 파일/폴더 변조	악성코드 전파	
임직원 계정 도용	시스템 파일과 유사한 파일명 사용	스케줄러 등록	
시스템 계정 도용	파일 삭제	인증된 바이너리 활용	

“Attack Lifecycle 정리”

“기업을 공격하는 가장 많이 사용되는 TTPs 확인 가능 ”

TTPs Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Spearphishing Attachment	User Execution	Scheduled Task	Scheduled Task	Process Injection	Credentials in Files	System Information Discovery	Remote Desktop Protocol	Data from Local System	Commonly Used Port	Data Encrypted	Endpoint Denial of Service
Valid Accounts	Scheduled Task	Create Account	Process Injection	Valid Accounts	Two-Factor Authentication Interception	System Network Configuration Discovery	Remote File Copy		Uncommonly Used Port	Exfiltration Over Command and Control Channel	Indicator Removal on Host
Replication Through Removable Media	PowerShell	New Service	New Service	Signed Binary Proxy Execution		System Network Connections Discovery	Replication Through Removable Media		Remote File Copy	Data Compressed	Inhibit System Recovery
Drive-by Compromise	Service Execution	Valid Accounts	Valid Accounts	Scripting		Account Discovery	Third-party Software				Resource Hijacking
Supply Chain Compromise	Signed Binary Proxy Execution	Registry Run Keys / Startup Folder	Web Shell	Rundll32		System Owner/User Discovery					Data Encrypted for Impact
Trusted Relationship	Scripting	Web Shell	Bypass User Account Control	Signed Script Proxy Execution		Process Discovery					
Spearphishing Link	Dynamic Data Exchange	Modify Existing Service		Bypass User Account Control		Software Discovery					
	Exploitation for Client Execution	Browser Extensions		Disabling Security Tools		File and Directory Discovery					
	Execution through Module Load	Hidden Files and Directories		File Deletion		Remote System Discovery					
	Rundll32			File and Directory Permissions Modification		Domain Trust Discovery					
	Signed Script Proxy Execution			Hidden Files and Directories							
	Third-party Software										

시작하기

Attack Lifecycle

+

TTPs Matrix

Threat Hunting에 기본이 되는
Data Set 구성

“ 공격 시나리오를 만들어 내는 밑 바탕”

시작하기

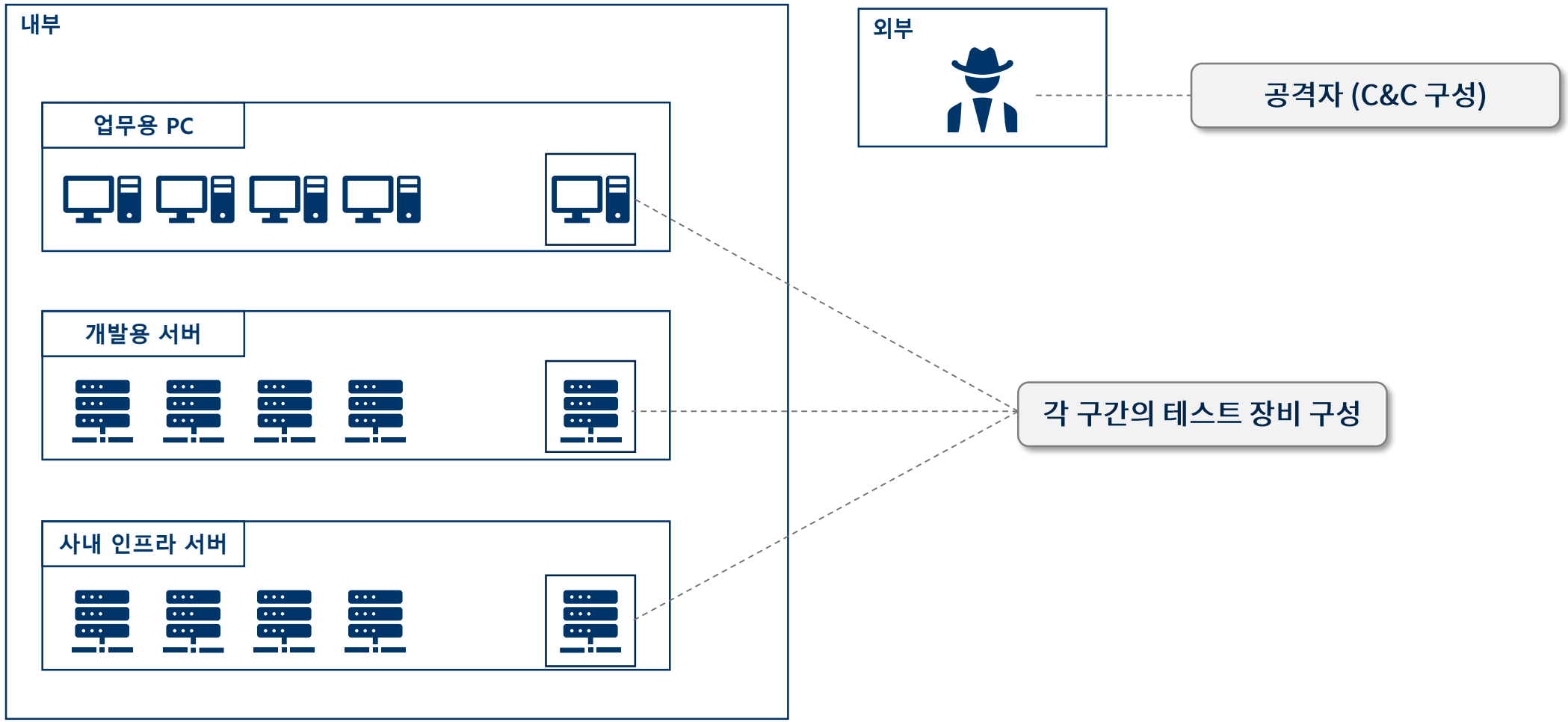
공격자처럼 생각하고!

공격자처럼 행동 한다.

“ Attack Lifecycle 과 TTPs 활용하여
공격 시나리오를 만들고 기업 인프라에 공격적인 테스트를 진행”

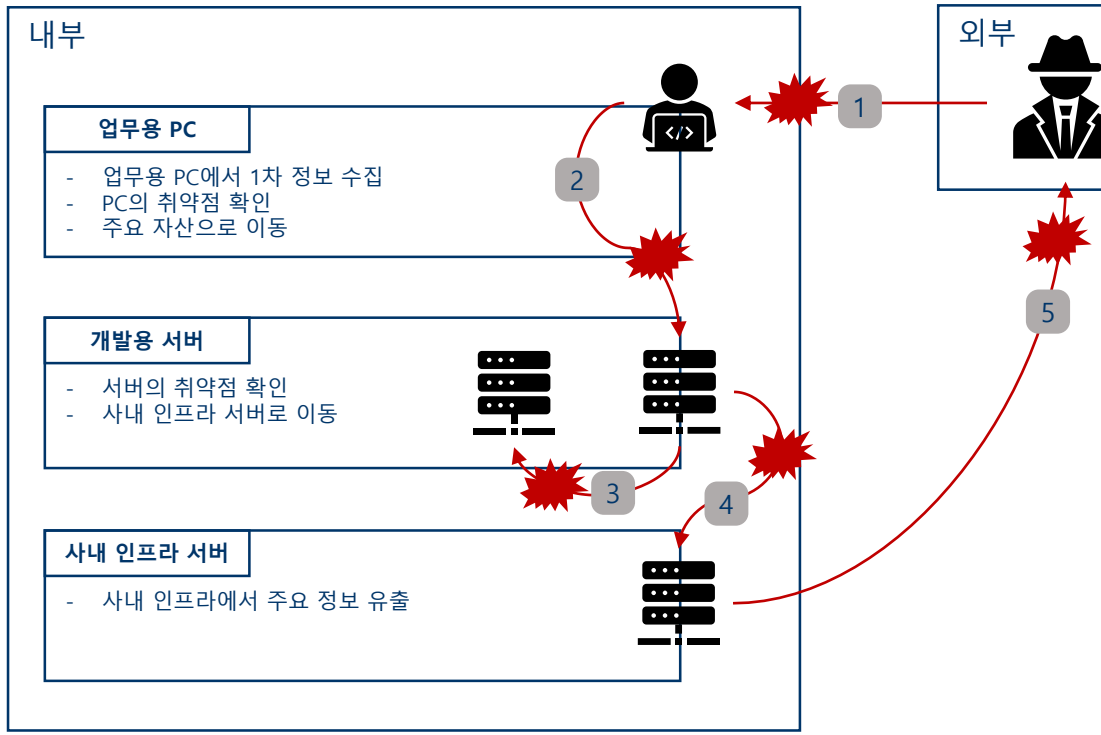
시작하기

우리 환경에 맞는 테스트 환경 구축



시작하기

SC-001



일반 적이지만 가장 위협적인
APT 형태의 내부망 공격 시나리오

NC Attack LifeCycle

초기 접근	장악	확산	목적 달성
Spearphishing Attachment	Scheduled Task	Account Discovery	Data from Local System
User Execution	Commonly Used Port	Bypass User Account Control	Exfiltration Over Command and Control Channel
	System Information Discovery	Uncommonly Used Port	Endpoint Denial of Service
	System Network Configuration Discovery	Process Injection	
	System Network Connections Discovery	System Owner/User Discovery	
	PowerShell	Process Discovery	
		System Network Configuration Discovery	
		System Network Connections Discovery	
		Remote System Discovery	
		Software Discovery	
		File and Directory Discovery	
		Credentials in Files	
		Remote Desktop Protocol	
		Create Account	
		Remote File Copy	
		Commonly Used Port	
		Scheduled Task	
		New Service	
		Service Execution	
		PowerShell	
		Valid Accounts	

시작하기

“ 공격자 처럼. ”

- 취약점 탐색
- 방어 우회
- 권한 상승
- 정보 악용
- 그 외 다양한 공격

E-mail 솔루션을 어떻게 우회 하지?

백신에 탐지가 되지 않도록 하는 방법은?

보안 정책 설정을 우회 할 수 있는 방법은 ?

최상위 관리자 계정을 탈취 할 수 있는 방법은 ?

결과

“ 테스트를 한 결과는 ? ”

“ 해본 것과 안 해본 것의 차이

공격 테스트를 통해 많은 것을 확인 했습니다. ”

결과

취약점

우회 기법

공격 기술

반드시 필요한 Action

내부 이벤트 전수 조사

“ 우리가 알지 못했던 취약점과

우회 기법에 의한 침해 징후는 없었다.”

탐지 강화로 빠르게 탐지 가능!

결과

“ 안전 하다고 생각 했던 곳에서 발견 된 설정 미흡”

당연하다고 생각했지만 당연 하지 않았다.

“ 설정 상태 재확인 및 설정 강화”

빠른 조치가 힘들 다면
위협을 빠르게 탐지 하도록 모니터링 강화

문제를 발견하고 해결하면서, 보다 안전한 업무 환경을 만들어 나갈 수 있다.

결과

탐지 개선

가시성 확보

보안 설정 강화

실제적이고 위험도가 높은 취약점을 찾아 조치 할 수 있는 체계 수립

데이터 수집 현황 및 상태 확인 가능

추가적으로 수집이 필요한 데이터와 모니터링이 필요한 곳 확인

APT 등에 대한 고도화 된 공격을 탐지 해내고, 이를 통해 공격 탐지시간을 지속적으로 단축함

결과

Attack Lifecycle

TTPs Matrix

공격시나리오 생성을 위한 Data Set

Attack Simulation

실제적인 위협 발견

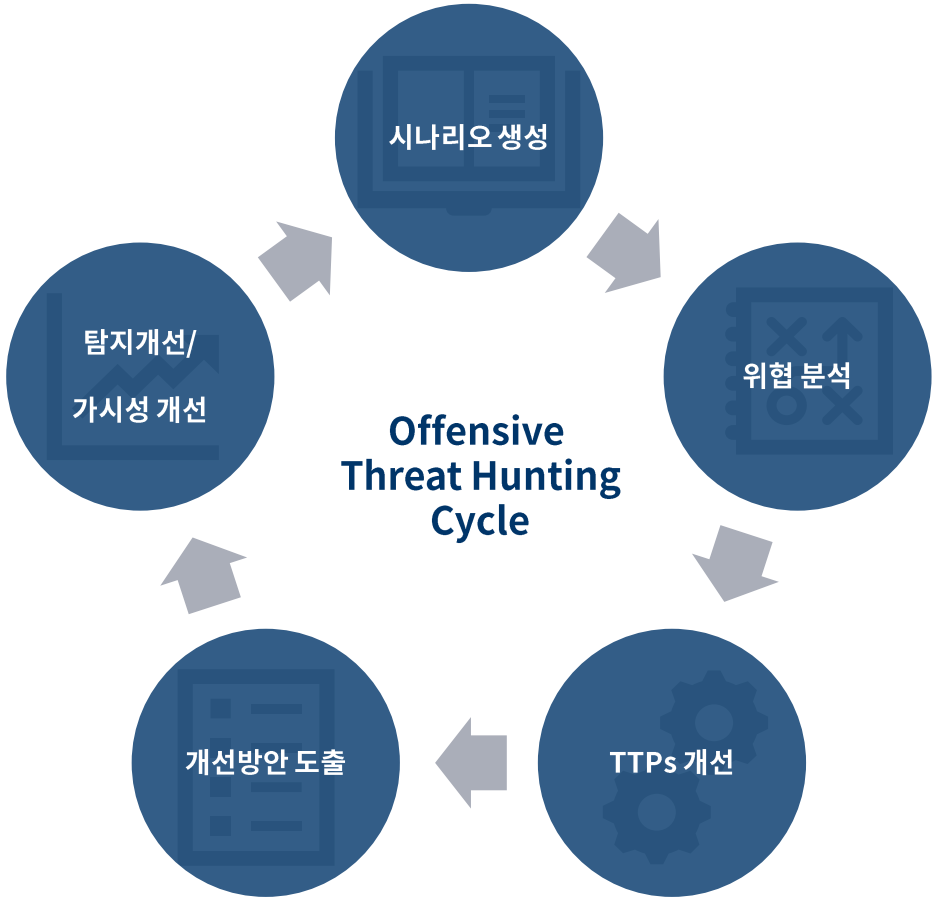
Threat Hunting

침해징후 발견 및 보안 대응 강화

“Offensive Threat Hunting”

결과

Offensive Threat Hunting Cycle



- 시나리오 생성
  - 외부 침해 사례, APT 공격 그룹 분석, 공격 기법 조사
  - 공격자 입장의 시나리오 생성
- 위협 분석
  - 실제적인 공격 시도
- TTPs 개선
  - 부족한 TTPs 추가/변경
- 개선 방안 도출
  - 탐지 및 인프라 문제 점 확인
- 탐지개선/가시성 개선
  - 도출 된 문제 점 개선

결론

“ 실제 기업에서 발생한 사고를 분석하면서 시작하는 것은 매우 좋음 ”

“ 분석할 시간적 여유가 없다면 해외 정리된 기법을 활용 하는 것도 좋다. ”

ATT&CK™ Evaluations

red canary Atomic Red Team

“ 한번 만이라도 사내 대상으로 테스트를 해보십시오
만족스러운 결과를 얻을 수 있을 것입니다.”

END OF DOCUMENT