# INCIDENT RESPONSE

leemon

20.05.12

# INDEX

# What Is IR

Event VS Incident


# What Is IR

## A – V – T – R Model

Asset Vulerability Threat Risk

# What Is IR

# A – V – T – R Model

## Asset

- 조직 내의 보호가 필요한 유형/무형의 모든 객체를의미합니다.
  - 유형 (조직원, 외주 직원, 고객, 서버 등)
  - 무형 (회사 평판, 주요한/민감한 사내 데이터, 소스코드 등)

# What Is IR

# A – V – T – R Model

## Vulerability

- 위협에 의해 권한 없이 무단으로 사용될 가능성이 있는 자산이 갖고 있는 기술/정책/관리적인 약점
  - 회사 홍보 목적으로 사용하는 사내 웹서버에 SQL 취약점이 존재
  - 사내 특정한 자산들에 제로-데이 취약점 공개

# What Is IR

## A – V – T – R Model

Asset Vulerability **Threat** Risk

- 취약점을 악용하여 자산에 접근/손상/파괴하려는 모든 시도
  - 권한 없는 조직원이 사내 민감한 정보 접근 시도
  - 사내 이메일을 통해 수신되는 모든 악성 메일
  - 인터넷에 공개된 제로-데이, 원-데이 취약점을 이용한 공격 시도

# What Is IR

# A – V – T – R Model

Asset Vulerability Threat Risk

- 사내 자산에 존재하는 취약성에 대한 악용 위협으로 인한 자산 손실,손상 또는 파괴 가능성
  - sql injection 취약점이 존재하는 웹서버에 대한 공격 시도로 사내정보 유출 및 위변조
  - 조직원이 사내 메일을 통해 수신된 악성 첨부파일 실행

# What Is IR

## A – V – T – R Model

Asset + Vulerability + Threat = Risk

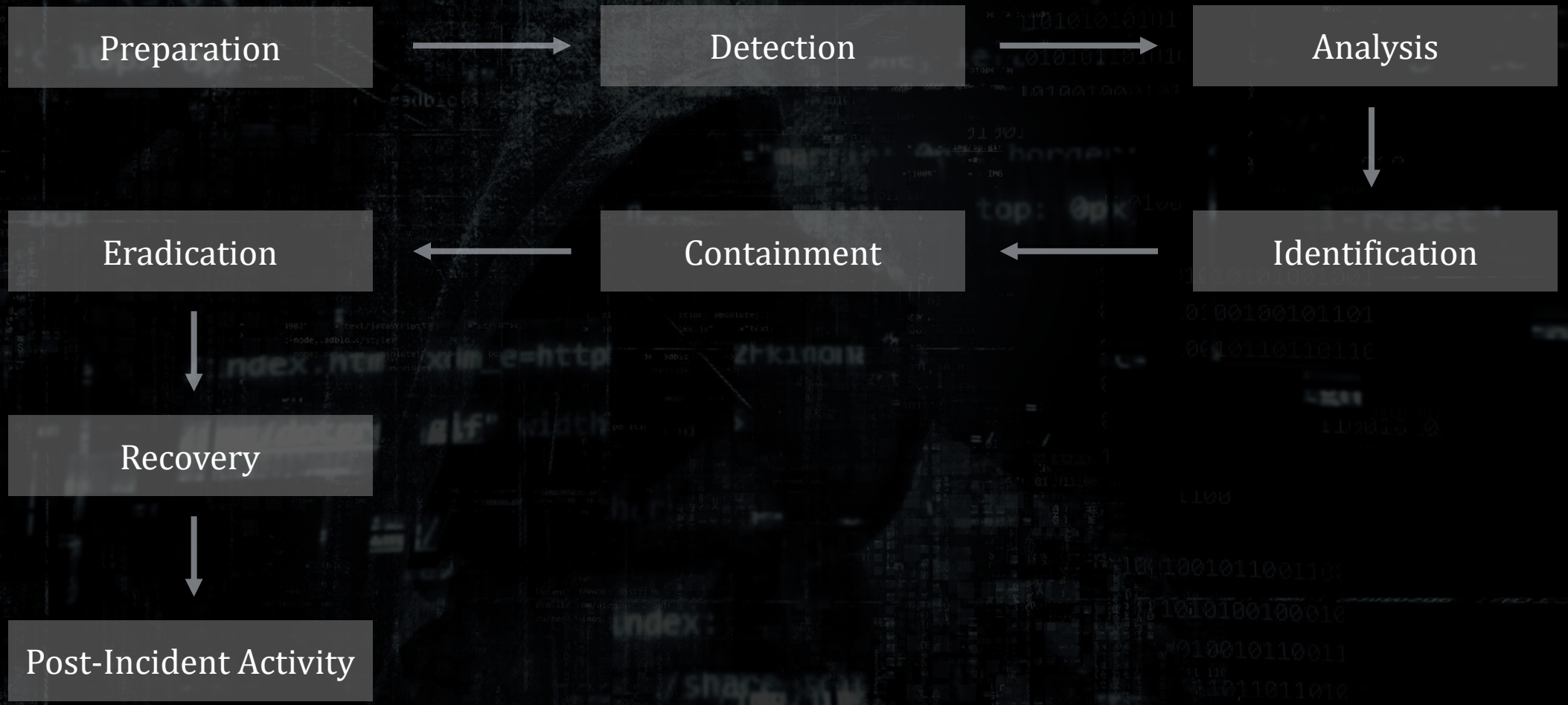
자산 내에 존재하는 취약성을 악용한 위협으로 발생하는 실질적인 손해와 그 가능성을 위협이라고 한다.

# What Is IR

## 침해사고대응(Incident Response)

- 침해사고에 효율/효과적으로 대응하기 위한 조직 실정에 맞는 실질적인 대응지침 수립
- 조직의 자산에 존재하는 취약성에 대한 위협으로부터 사고발생시 위험을 완화 하도록 지원
- 침해사고를 막는다는 개념보다는 완화(Mitigation) 하는 개념에 집중한다

# IR Process


Preparation
Detection
Analysis
Identification
Containment
Eradication
Recovery
Post-Incident Activity

# IR Process

Preparation

Detection

Analysis

Identification

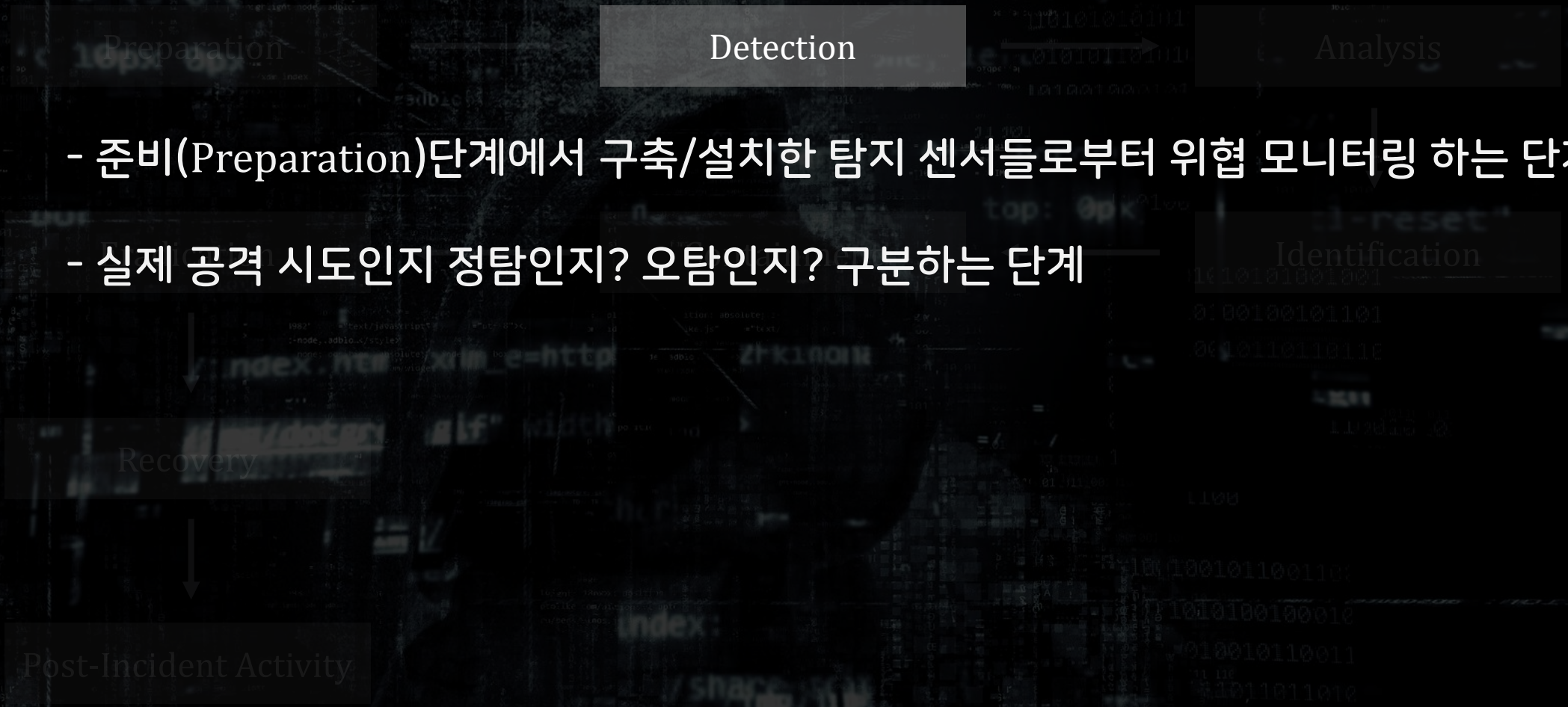
Recovery

Post-Incident Activity

- 침해사고대응을 위한 정책/계획/절차/지침을 수립하는 단계

- 침해사고대응을 위한 탐지 센서 구축/설치하는 단계

# IR Process




- 준비(Preparation)단계에서 구축/설치한 탐지 센서들로부터 위협 모니터링 하는 단계

- 실제 공격 시도인지 정탐인지? 오탐인지? 구분하는 단계

# IR Process

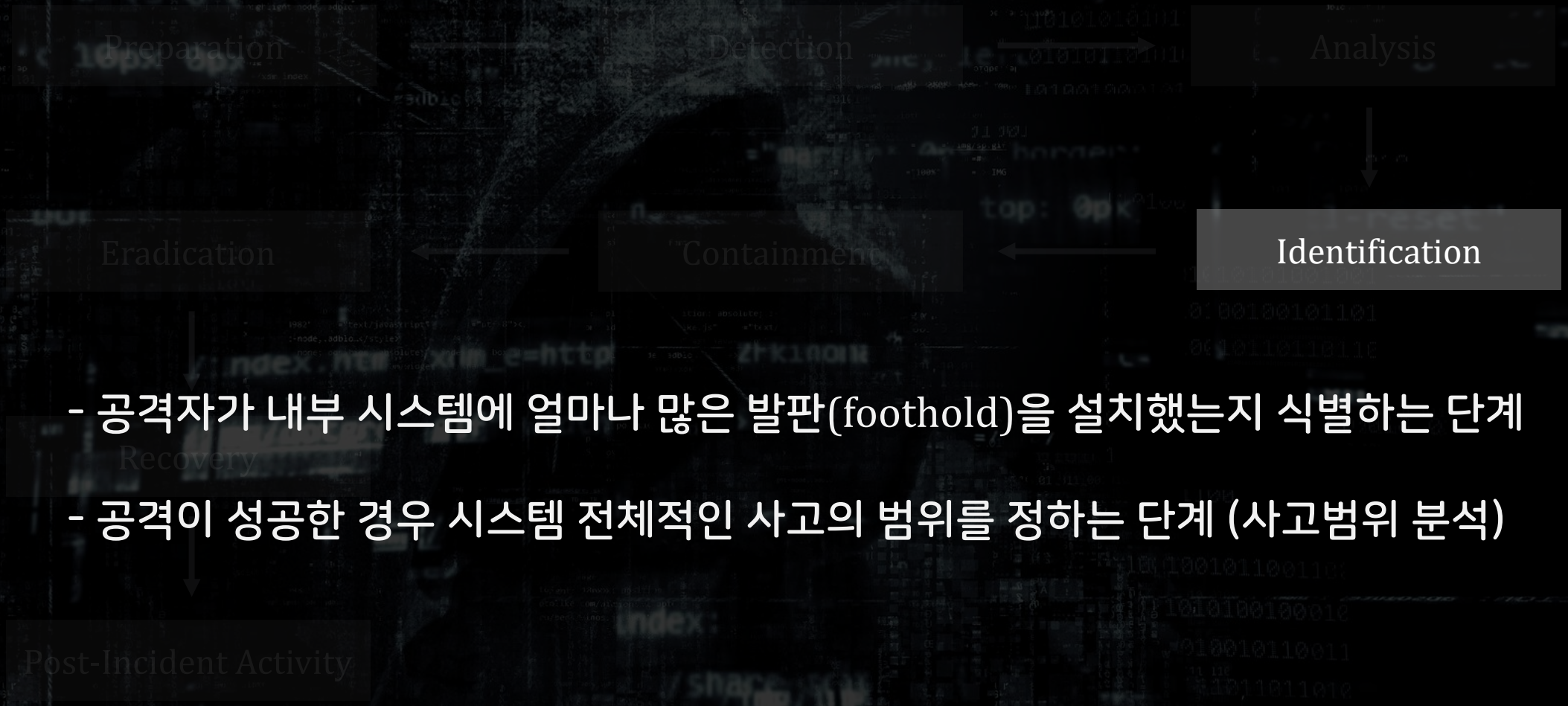
Preparation → Detection → Analysis

- 내부 자산에 대한 위협이 실제로 취약성에 위험을 발생시켰는가?
- 실제 공격이 성공한 호스트에서는 어떠한 일이 발생했는가? (영향도 분석)
- 얼마나 심각한 공격이 성공했는가? (심각도 분석)

Recovery

Post-Incident Activity

# IR Process




- 공격자가 내부 시스템에 얼마나 많은 발판(foothold)을 설치했는지 식별하는 단계
- 공격이 성공한 경우 시스템 전체적인 사고의 범위를 정하는 단계 (사고범위 분석)

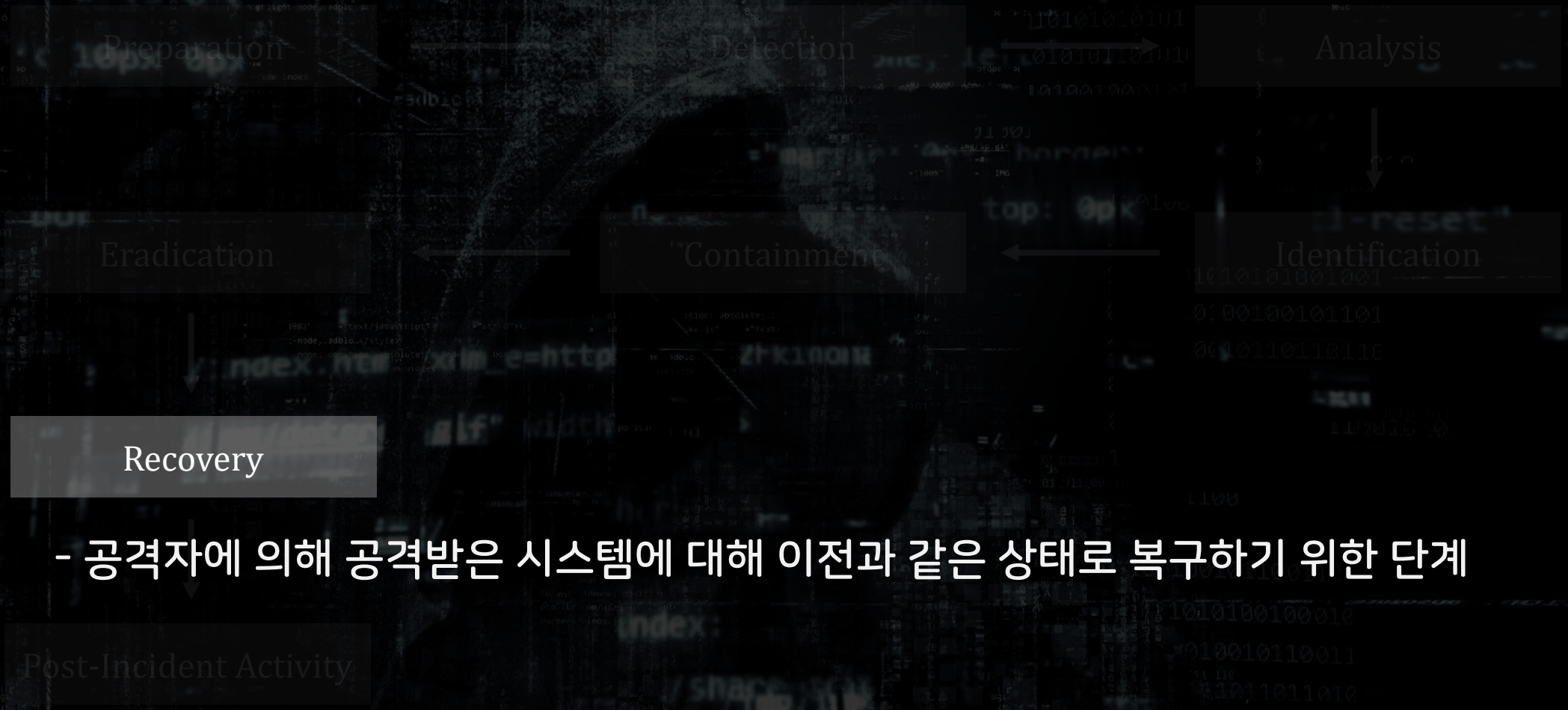
# IR Process


- 다른 시스템이 추가 점령/감염/전파되는 것을 막기 위한 단계
- 식별(Identification)단계를 통해 파악된 사고의 범위를 통해 격리범위 판단 가능
- 현실적으로 완벽히/신속히 수행되기 매우 어려운 단계

# IR Process


- 공격자가 내부 시스템에 설치한 발판(foothold)들을 제거하는 단계
  - 침해된 사용자 계정 비활성화/삭제
  - 악용된 취약점/서비스 제거

# IR Process




- 공격자에 의해 공격받은 시스템에 대해 이전과 같은 상태로 복구하기 위한 단계

# IR Process


- 사고 원인을 다시 추적/분석하며, 놓친 부분이 없는지 재확인하고 보고하는 단계

Post-Incident Activity

# Initial Access

## 초기침투(Initial Access)

- 조직 네트워크 내에 초기 발판(foothold)을 확보하기 위한 기술

# Initial Access

## Spearphishing  Attachment/Link/via Service

- 특정 개인, 조직 또는 비즈니스를 대상으로 하는 전자메일 또는 전자통신 사기
- 악성객체를 열어보게끔 그럴듯한 유혹으로 기만
- 난이도가 낮지만 가장 많이 성공하는 공격이며, 공격자가 애용함

# Initial Access

## Spearphishing  Attachment

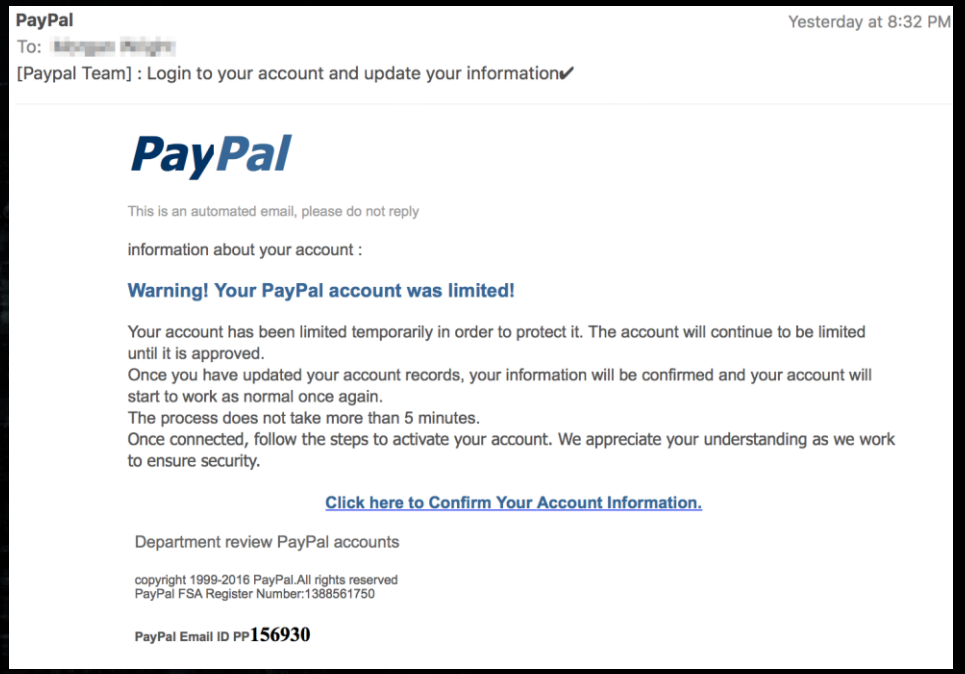
- Spearphishing 메일에 악성파일 첨부하는 방식
- MS Office, PDF, ZIP, HWP 등 많은 옵션 존재

Spearphishing 메일에 악성링크 첨부하는 방식

# Initial Access

## Spearphishing Link

- Spearphishing 메일에 악성링크 첨부하는 방식
- 악성링크에는 다운로드링크 혹은 익스플로잇 코드 링크를 포함한다.



PayPal Yesterday at 8:32 PM

To: [redacted]

[Paypal Team] : Login to your account and update your information✔

PayPal

This is an automated email, please do not reply

information about your account :

**Warning! Your PayPal account was limited!**

Your account has been limited temporarily in order to protect it. The account will continue to be limited until it is approved.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.
Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

Click here to Confirm Your Account Information.

Department review PayPal accounts



PayPal Email ID PP156930

Spearphishing 메일에 악성링크 삽입 하는 방식

# Initial Access

## Spearphishing  via Service

- 조직 내부 메일 주소가 아닌 타사 서비스로 Spearphishing
- 일반적으로 SNS 등을 통해 친분관계 형성후 악성객체 전달

# Execution

## Execution

- 공격자는 내부 네트워크에서 악의적인 코드를 실행
- 로컬 또는 원격 시스템에서 악의적인 코드를 실행하는 기술로 구성

# Execution

## PowerShell

- 정상 용도
  - Windows 운영체제에 포함된 가장 강력한 인터페이스
- 악의적 사용
  - 공격자는 정상 명령행을 악용; 정보탐색; 코드 실행 등 수행
  - 원격 시스템 연결 가능
  - 인터넷에서 다운로드 및 실행 가능

# Execution

Practice


Q & A