

Week 1: Breach Response Case Studies.

NIST Computer Security Incident Handling Guide

Actions :-

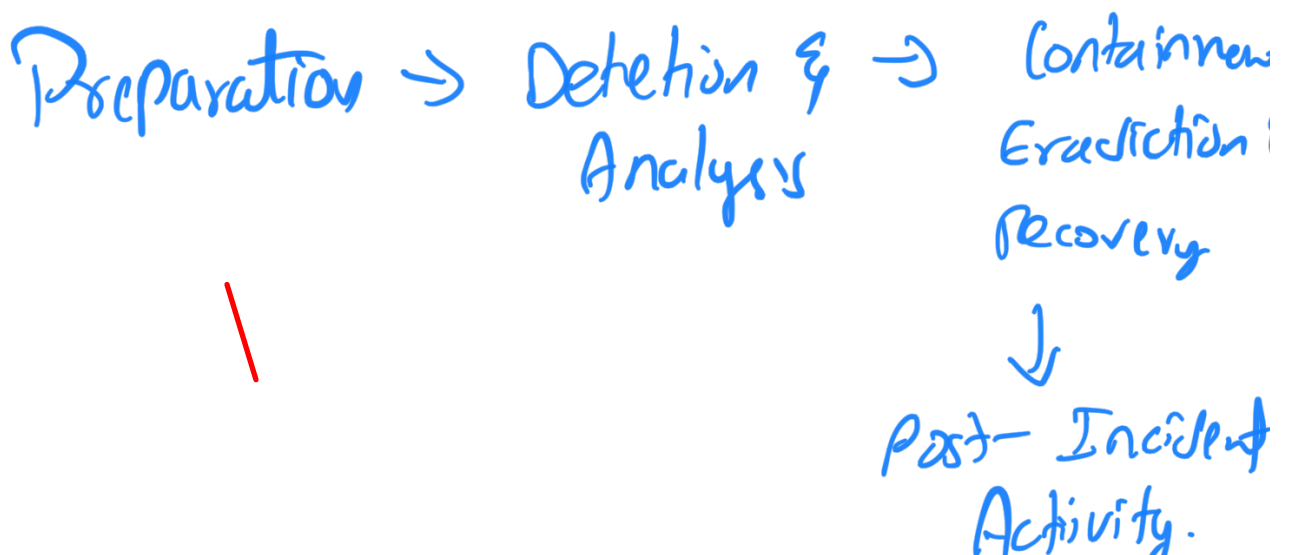
- 1.) Establish a formal incident Response policy.
 - 2.) Create an incident response policy
 - 3.) Develop an incident response plan based on the incident response policy
 - 4.) Develop incident response procedures
 - 5.) Establish policies and procedures regarding incident-related information sharing.
- It is important to have a plan in place when

6) Consider the relevant factors in selecting an incident response team model

Incident Response Team Structure

- 1.) Team Model
- 2.) Team Model selection → Onsite using Third Party.
- 3.) Incident Response Personnel
- 4.) Incident Response Team Services.

NIST Incident Response Lifecycle



What is a Breach?

A data breach is the result of another security incident, whether it is an attack by hacker, a careless or malicious insider, or even an accident involving faulty processes or procedures.

Data Breach → Organization Only

↳ Data inside and outside of the organization

↳ Technical Aspects.

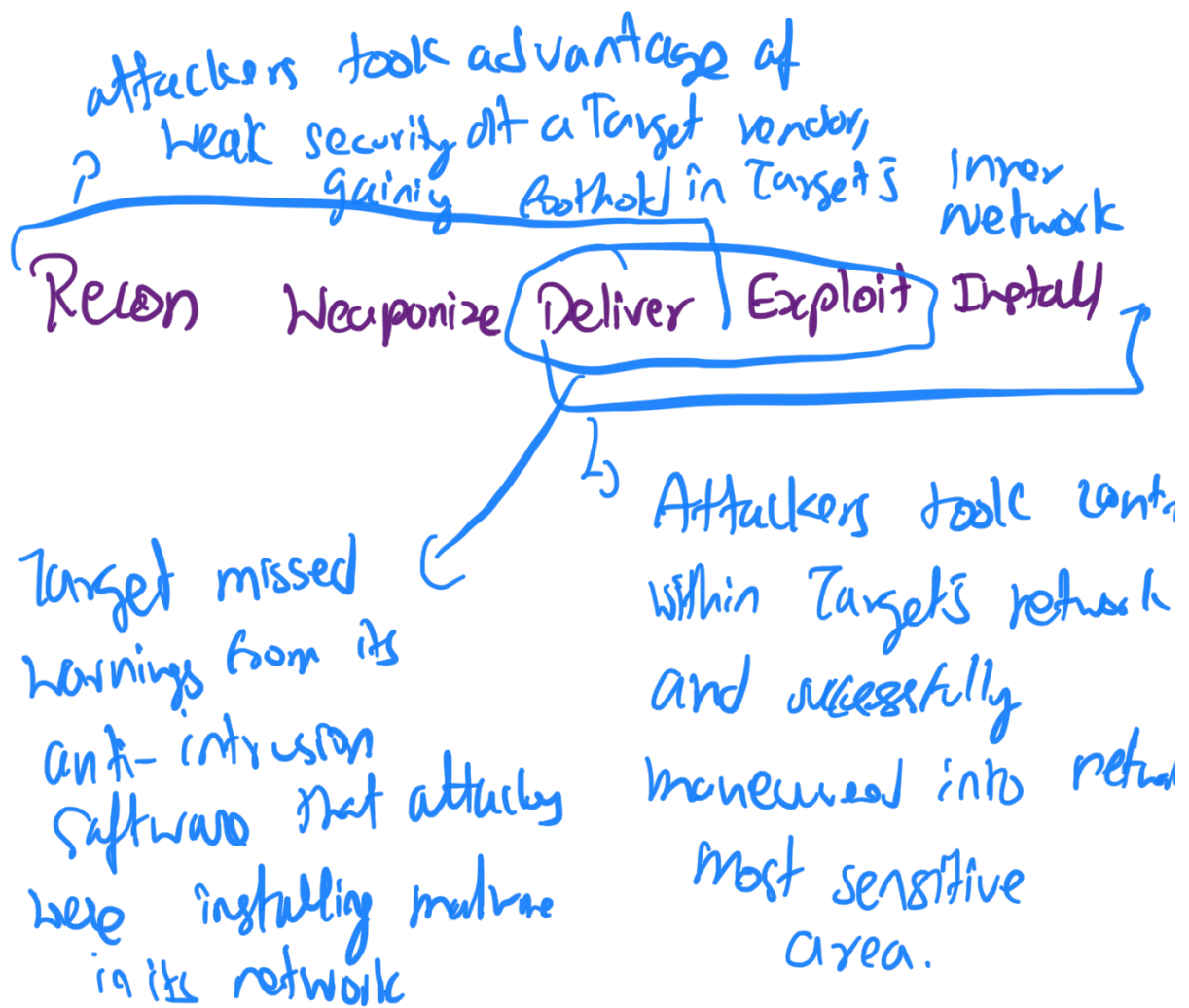
↳ Communications.

Who should be involved?

→ Management team

- legal personnel
- Public Relations

Target Attack Timeline → Kill chain Timeline



Command & Control → Action

↓
Target missed information provided
by its anti - intrusion software
about the attackers
escape plan, allowing attackers
to steal as many as
110 million customers records

Prevention

- Security logs & events
- Network Flow of Data
- Vulnerability data
- Network Topology
- Asset profile with business context, risk, ownership.
- User behaviour Analysis

- Increased Incident Reports.
- One Incident case of Analysis
- Massive Reduction of Window of exposure.