Incident response policy

- Preparation
- Identification
- Containment — Segmentation/communication
- Eradication
- Recovery
- Post-incident activity

Cyber Incident response teams

Reporting, Categorizing and priortizing (triage)

↳ Incident analysis

CIRT	cyber-Incident response team
CERT	computer emergency response team
CSIRT	computer security Incident response team
SOC	security operations center

24/7 availability

Roles beyond technical response

- legal
- HR
- Marketing

Communication Plan and Stakeholder Managment

- Must make sure not to inadvertently disclose Info to Parties that do not need to know. you can avoid this by the use of call lists

- Call list:
  A list of authorised people to notify

- Communication plan
  - Share data on a need to know basis
  - Use out of band communication to avoid alerting Intruder. (Signal, etc)

- Stake holder managment
  - Communication with Internal / External stake holders.
  - reporting and notifying

Incident response plan

- Lists procedures, contacts and resources available to respond to different types of attacks.

- Play books and runbooks (USE SIEM Reports)
  - Guides for junior analyst to follow (Based on type of attack)

- Incident categorisation

- Priotizing Incidents based on

- Data Integrity
- Down time
- Economic / Publicity
- Scope
- Detection time
- Recovery time

Cyber kill chain Attack Frame work

1- Recon

2- Weaponization

- Coupling exploit w/ Vulnerability

3- Delivery (of payload)

4- Exploitation (running exploit)

5- Installation

- Acheiving persistance
- RCE

6- Command and Control

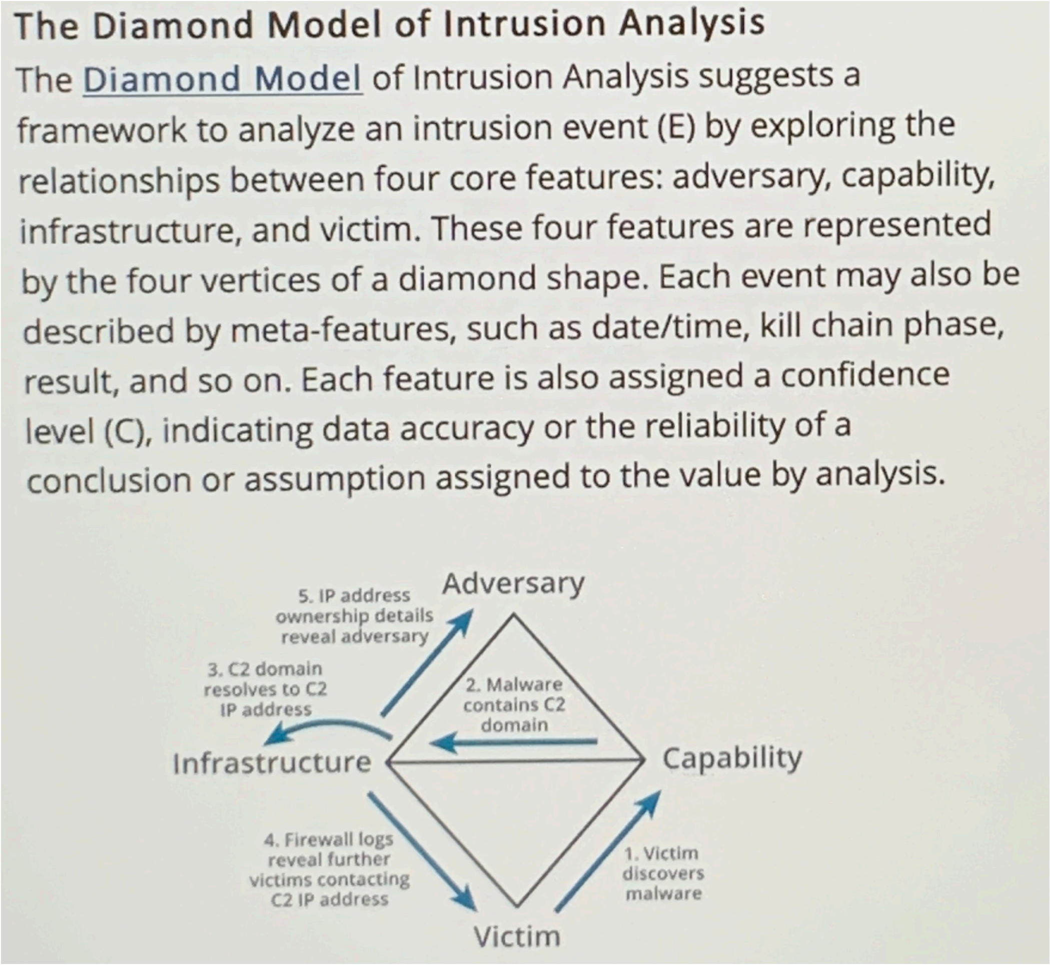
7- Actions to achieve objectives e.g data exfilteration

Other Attack frame works

MIRE ATT&CK

- Matrices that provides access DB of TTP (each technique is given an ID #)
- Tactic categories (Recon, Exf ....)
- No explicit sequencing (must figure that out on your own)

The diamond model of Intrusion analysis



The Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis suggests a framework to analyze an intrusion event (E) by exploring the relationships between four core features: adversary, capability, infrastructure, and victim. These four features are represented by the four vertices of a diamond shape. Each event may also be described by meta-features, such as date/time, kill chain phase, result, and so on. Each feature is also assigned a confidence level (C), indicating data accuracy or the reliability of a conclusion or assumption assigned to the value by analysis.

1. Victim discovers malware
2. Malware contains C2 domain
3. C2 domain resolves to C2 IP address
4. Firewall logs reveal further victims contacting C2 IP address
5. IP address ownership details reveal adversary

Incident Exposure Exercises

- Table top
  - Scenario based (not live)
  - cheapest one
- Walk through
  - Responders demonstrate response actions
- Simulation

  Red vs Blue teams

Incident Response, disaster recovery, Retention policy, business continuity

- Disaster recovery plan (large # of stake holders/ resources)

  (may Involve moving data to a secondary location)
- Business continuity plan (BCP)

  How the business will deal with a minor or major incedent
- Continuity of operation planning (COOP)

  like BCP but for goverment. specifies back up methods w/out IT support

Incidence response, forensics and retention policy

- Digital forensics requirments
- Retention policies for evidence storage