7. Threat Intelligence

I. Types of Threat Intelligence

- Strategic
  - High level analysis
  - Trends, risks, impacts
  - Threat Actor motives, goals, capabilities
  - Deciding long-term security strategy
- Tactical
  - Tactics, Techniques, Procedures (TTPs)
  - Threat actor behavior and methodologies
- Operational
  - Imminent threats, plans, timelines
  - Tracking threat actors and groups
- Technical
  - Tools, infrastructure, technical capabilities
  - IOCs
  - Integrate into tooling to enhance detection

II. Threat Intelligence Cycle

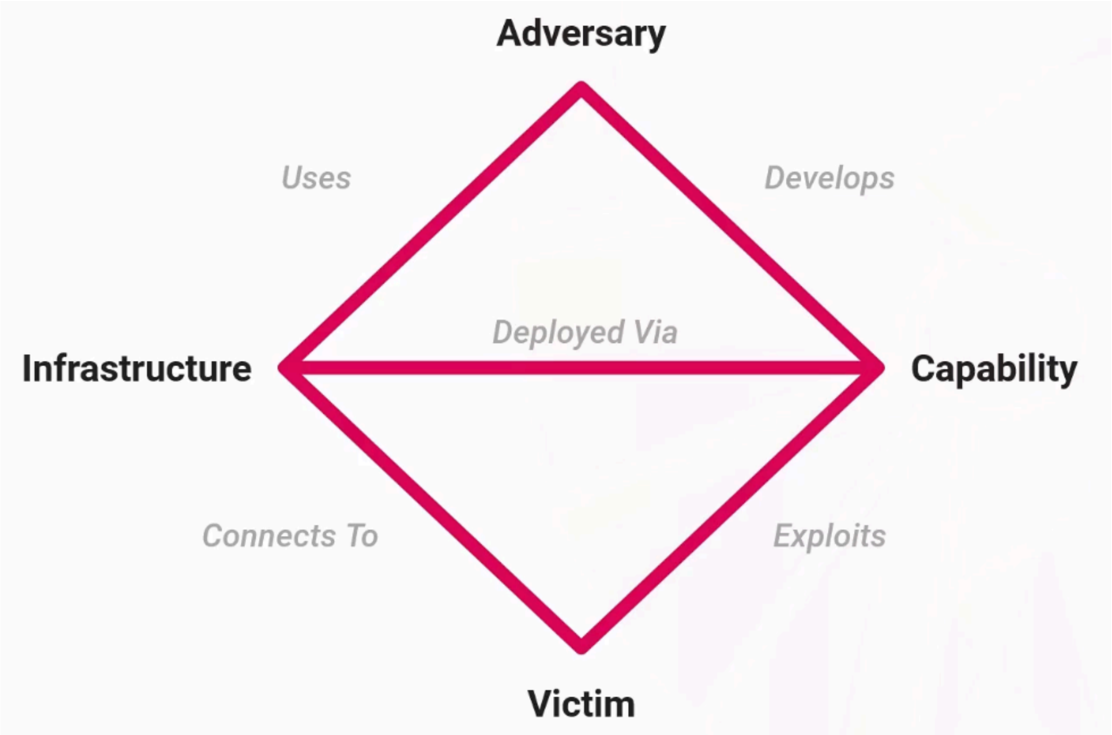
1. Planning: Requirements and Direction
2. Processing: Collect relevant data
3. Analysis
4. Dissemination
5. Feedback

Intelligence Sources

- OSINT - Open-Source Intelligence
  - Dark web, forums, social media
  - Passive recon, vulnerability, malware databases
  - Public repositories

- Commercial Threat Intel
  - Third party vendors
  - Proprietary subscription-based threat feeds
- Vendor Reports
  - Published reports and white papers
- Information Sharking and Analysis Centers (ISACs)
  - Industry groups facilitating TI sharing

III. Diamond Model of Intrusion Analysis



- Adversary
- Capability
- Infrastructure
- Victim

IV. The Cyber Kill Chain

1. Recon
2. Weaponization

3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

V. The Pyramid of Pain

Causing Pain to the Hackers

1. Hash Values
   a. Trivial to replace
2. IP Addresses
   a. Easy to change to a new IP
3. Domain Names
   a. Simple for a hacker to switch to a new domain
   b. Networks can block domains registered < 30 days
   c. Hackers would need to have prebuilt domains before starting
4. Network / Host Artifacts
   a. Annoying for hackers to have to change
   b. registry keys
   c. downloaded files
   d. User-Agents
   e. They won't know what got detected and will have to keep rebuilding
5. Tools
   a. Challenging for a hacker to switch to a new tool
6. TTPs
   a. Tough to change
   b. Determine what behavior got caught or find another target

VI. YARA

VI. MISP - Malware Information Sharing Platform

Threat Sharing Protocols

- STIX - Structured Threat Information Expression
- TAXII