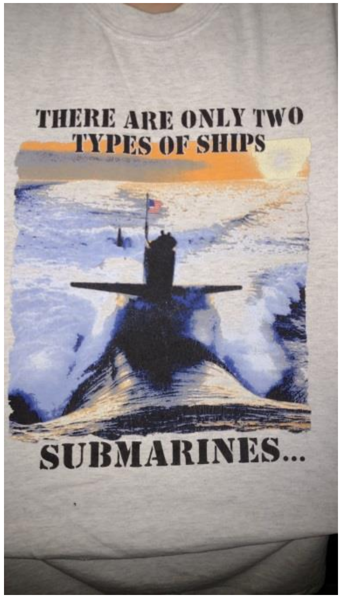
Defense in Depth is more critical than ever

Depth Charges

Donald Warnecke
MAOM, CISSP, GCIH

Who am I

- 20 years in IT and Security services
- Degrees: MAOM, BS, AB
- CISSP, GCIH, GSNA, GICSP
- Previously held CCNA, CCSE, ISS-SE
- DoD and Utility industry
- Strength-based leadership



Agenda

- Defense in Depth
- Sliding Scale of Cyber Security
- Implementation & Systemic Barriers
- Use Cases

1. Defense in Depth Backstop

The coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise.

Image: http://consider-ations.blogspot.com/2010_12_01_archive.html

2. Defense in Depth Onion

An IA concept in which multiple layers of security controls are placed throughout an information technology (IT) system.

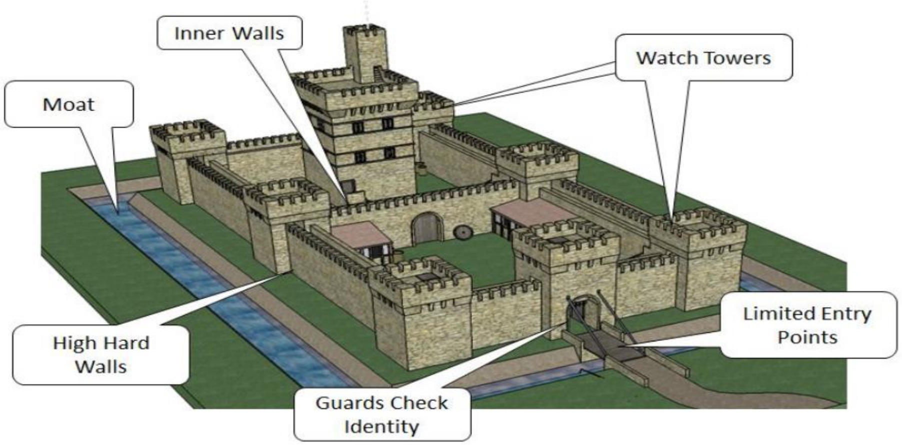


Image: http://www.socialengineeringblogs.com/category/physical-security/

DiD Time Equation

$$T_D + T_R < T_F$$

Time to Detect an event (T_D)

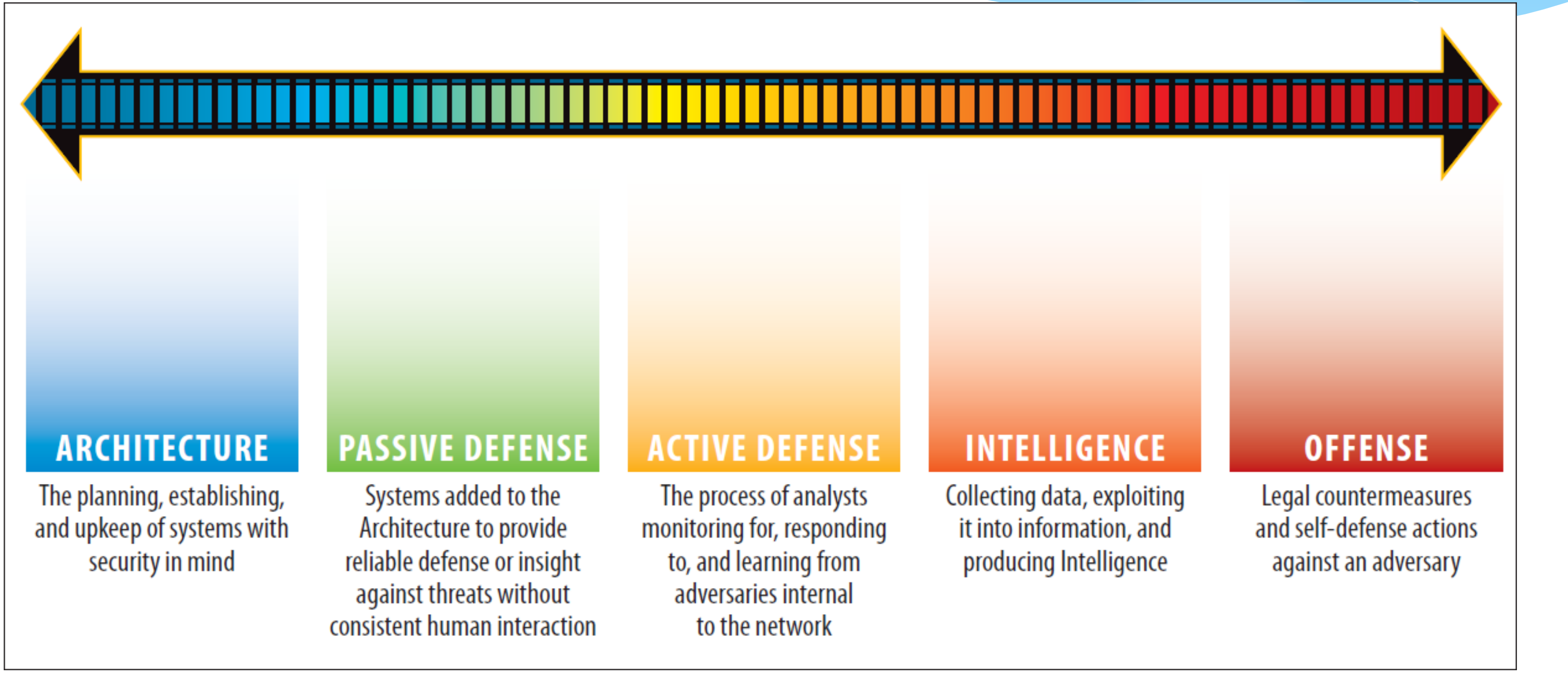
+

Time to Respond an event (T_R)

<

Time to Protection Breach or Failure (T_F)

Sliding Scale of Cyber Security



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

Implementation & Benefits

- Distinct components
- Bottlenecks of defense
- Selective, increased awareness

Common Barriers

- Lack of asset identification
- Manpower
- Philosophical mismatch

Use Case 1

- Full: Significantly limit network traffic
- Partial: Alert on certain kinds of traffic
- Small: Well-defined permitted traffic

Use Case 2

- Full: Changes to groups and users
- Partial: Administrative object changes, unknown user
- Small: Distinct accounts, default user

Use Case 3

- Unexpected intranetwork communication

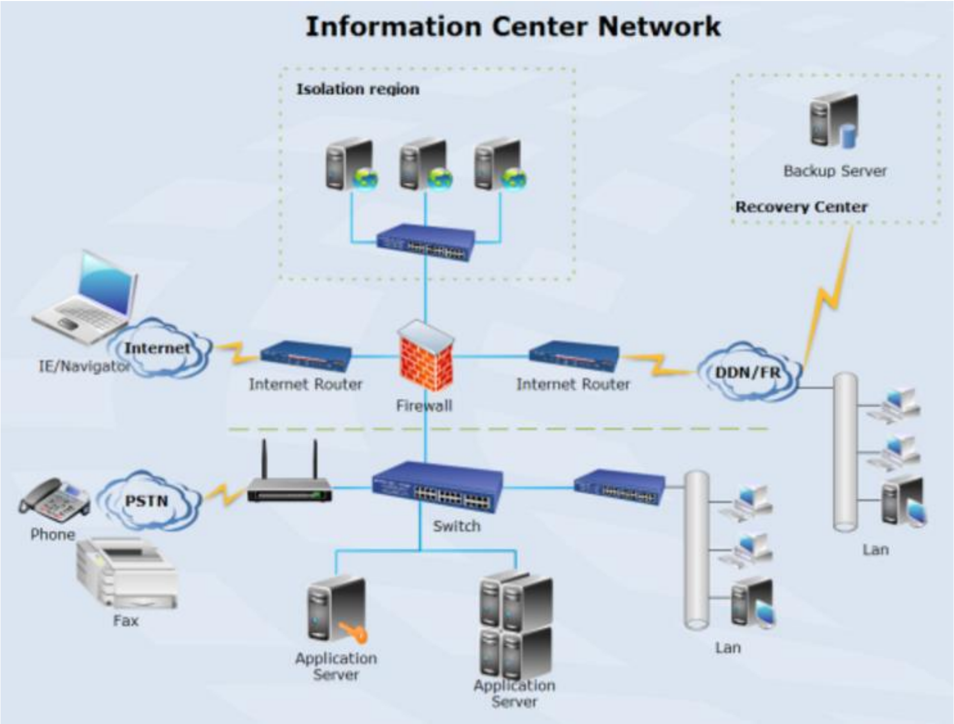


Image: https://www.edrawsoft.com/Logical-Network.php

Hunting Leverages DiD

- Stronger understanding of high-value assets
- More threads to pull on
- Less noise

Summary

- Defense in Depth
- Sliding Scale of Cyber Security
- Hunting can leverage DiD

Questions

Thank you!