# Principles for Cyberwarfare

# Cybersecurity vs Cyberwarfare

**Why it is war**

- Advanced and Persistent Threat Actors
- Attacks intended to cause damage
- Attacks are always part of a larger chain
- Cyberwarfare threatens to halt Digital Transformations:
    - Singapore: 71%
    - France: 65%
    - UK: 64%
    - US: 54%
    - Germany: 50%
- And much more chaos not yet covered; it is truly a horrible idea to ignore/underestimate it

**Why it is not in general security**

- Few commonly used attacks utilized
- Attackers are dedicated towards single target/group of targets
- Frequently utilize large scale botnets nearby the target
- Only 52% IT admins admit havzng any form of a contingency plan
- Aims of attackers (employee survey):
    - Databases/PII: 54%
    - Intellectual property: 51%
    - Connected hardware and software: 47%
    - Operational downtime: 24%
    - Critical infrastructure: 19%

# Cybersecurity vs Cyberwarfare

## Cyber Warfare

- SIA Triad
- Investigating and Responding to Tactics, Techniques and Procedures
- For all digital assets

- Only for organizations and persons that are very significant and valuable
- Demand: Flexible Architecture powered by latest TI (eg. DDoS)

## Cyber Security

- CIA Triad
- In accordance with compliances and benchmarks
- For Data

- For all organizations and persons that regularly use any form of digital assets
- Demand: Genuine adherence to Cybersecurity GRC (eg. Chatbot)

"Our principles are the springs of our actions; our actions, the springs of our happiness or misery

- Philip Skelton

# 0.
# Flexible Security

The foundational principle

# About Flexible Security

- A security solution is only flexible if:
  - It is cost-affordable
  - It does not require heavy movement of specialized personnel
  - It is not very time-consuming to apply or modify
- Most security solutions are **not** flexible, instead fancy, expensive and complicated.

# Why Flexibility?

- Advanced Persistent Attackers:
  - Frequently Change TTPs, using Blitzkrieg in serious operations
  - **Will** break through each defence setup in a short time, if dedicated
  - Usually cause massive, maybe lethal damage to organizations

- Not being flexible = Too slow to save self

# 1.

# Defense in Depth

The first golden principle

# About Defense in Depth

- Imagine a Castle
- Each security mechanism fits perfectly with the others around it, like a jigsaw
- Rely on multiple low to no cost solutions over single expensive solutions

# An Example: Email Security

Business Email Compromise is a rising trend of Cyber Attacks today.

1. Email Gateway/Anti-Spam Filters
2. User Awareness Training
3. Automated Email Pullback
4. Multi Factor Authentication
5. Remote Browser Isolation
6. SSL Decrypting Firewall and NTA

# Case Study: Internet Archive

- Popular Website Internet archive runs a website called Wayback Machine, offering a view into cached content and site from even decades ago
- It was the subject of multiple DDoS attacks and an un-named JS library was hacked to reveal credentials of 31 million users
- The attackers attacked only because it was a US-based Non-Profit, and their political beliefs went against the United States.

# How DoD would enable response

DDoS:

- Utilize online website protections like Cloudflare (cheap and reliable)
- Ensure Server OS IPTables and Instance Firewall rules are as secure as possible
- Set-up specialized anti DDOS FOSS tools such as FastNetMon or DDOSMon

# How DoD would enable response

JS:

- Mandate MFA for logging into all accounts, and FIDO keys for admin accounts
- Build honeytokens into your code: Honeytokens are basically fake sensitive data that alerts owners and tracks attackers
- Encrypting all sensitive data (both username and password) with AES, not just salting

# 2.
# Least Privilege

The second golden principle

# Least Privilege Major Concepts

### Access Prevention

Only give access rights to people who are **both** authorized, and required access privileges.

Example: Sysadmin vs Network Engineer

### Hardening

Refers to **ruthlessly** cutting attack surface on systems. For example; regularly running nmap on your subnet to find un-necessary FTP ports etc.

### Privilege Creep

This refers to a situation when a person gains access without authorization or need; eg. Ex-employees, accidental access granted during promotion/demotion etc.

# Implementing Least Privilege

## Comprehensive Hardening

There are 2 ways to harden devices:

1. Using FOSS softwares (Eg. OpenWRT, PfSense etc.)
2. Referring to benchmarks such as NSA and DoDStig

## Access Prevention

Ensure default permissions are set to minimum.

This is best done using IAM tools (FOSS), such as OpenIAM, Keycloack etc.

These tools also provide ease of audit for periodic checks.

## Avoid Privilege Creep

This can be prevented by audits; either manually (eg. Re-Certification Programs) or with free automated tools such as IAM-Deescalate for AWS

# Case Study: MGM Resorts

- A famous hacker group found an IT employees' name, phone number and other details from LinkedIn; and looked up their contacts
- Used this data to spoof a call from his number to the MGM help desk and pretended to be him, tricking them into installing malware
- The attackers managed to lock down everything from hotel room doors to casino machines and even personal consumer data like SSNs

# How LP would prevent

- **Comprehensive Hardening:** By ensuring helpdesk employees use least vulnerable Operating Systems such as Linux, along with hardened built-in firewalls the malware may not have succeeded
- **Access Prevention:** Ensuring that helpdesk machines, room locks and casino are not on the same network may have stopped the lateral movement of attackers
- **Avoid Privilege Creep:** Ensuring that no employees have any kind of admin or cross-department access would further make privilege escalation and lateral movement very difficult

# 3.

# Reinforcement of Securities

The third golden principle

# About Reinforcement

- Imagine a Door to a bank locker
- This door has 2 very strong locks; even if one is stolen off the manager, the cracker must find who has the other key and steal it from them
- This increases pain of the attacker, making majority look elsewhere

# How it differs from DoD

- DoD applies layers of security
- For the bank locker example; DoD would say put one genuine door behind and one fake door with electric shock defence behind the first
- While DoD increases pain; DoD with reinforcement exponents it

# Implementing Reinforcements

Whenever implementing one layer of security mechanisms, implement another along with; for example:

1. Authentication with Keycloak + Authorization with Apache Shiro
2. VPN with OpenVPN + Firewall with iptables

# Case Study: CISA

- The Cybersecurity and Infrastructure Security Agency (CISA) — responsible for cybersecurity and infrastructure protection across all levels of the United States government, was hacked.
- By exploiting vulnerable Ivanti Connect Secure and Ivanti Policy Secure gateways; the hackers managed to compromise critical systems about Infrastructure Security and Chemical Terrorism

# How Reinforcement would prevent

- By not solely relying on tools from one organization, they could have also connected a network gateway to their router, the gateway utilizing security tools from more reliable companies like Fortinet, Cisco or Palo Alto
- Implementing FOSS or different NAC controls across gateways of different network segments alongside would have made it difficult for hackers to breach multiple departments

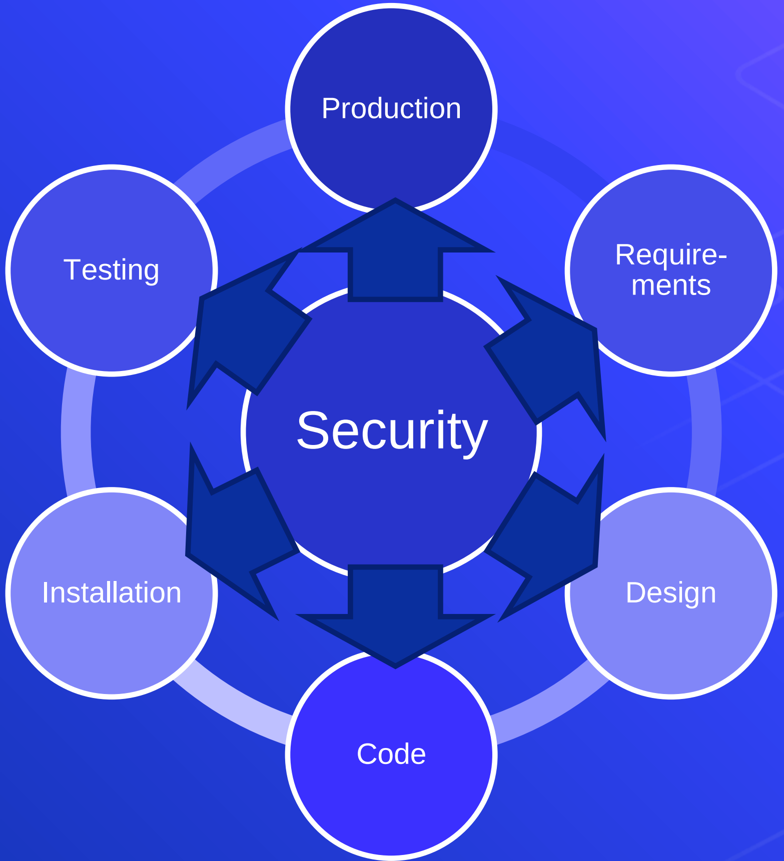
# 4.
# Secure by Design

The fourth golden principle

# About Security by Design

- Imagine a building in earthquake prone area
- We cannot make the building earthquake resistant after completing it
- Earthquake proofing must be incorporated in each step from blueprints to completion

# Security by Design



# Case Study: Healthcare in the U.S.

- Medical devices are generally not developed with cybersecurity in mind, but rather stability and efficiency
- Attacks for years have utilized this to deploy ransomware in critical systems like Ventilators, ICU systems etc.
- Many developed countries have adapted to it in some way or another, but the United States continues to be one of the worst hit.

# How SbD would enable response

- After realizing that the machines are going to be vulnerable, network engineers should try to secure the network segment gateway
- This can be done using FOSS routerwares or proprietary solutions; or even just Gentoo linux with really strong IPTables
- They may also setup admin accounts on the machines and MFA for those logins

There are infinite ways to do this; the important thing is to do it before deploying the machines.

# Zero Trust Architecture

# Why Zero Trust is not an all purpose solution

**Defence in Depth**

ZTA is a vague, all-encompassing principle; so in implementing it, most end up adding ad-hoc, non-supplementary checks and balances.

**Security By Design**

ZTA violates Security by Design, since it takes focus away from step by step security and replaces it with a “bolt on the door” system

**Least Privilege**

ZTA while seemingly working on least privilege, takes it to such an extreme that it causes employee burnout and bypasses/rollbacks.

**Pyramid of Pain**

ZTA violates pyramid of pain by reducing pain for attackers; the only thing they must focus on is authentication

**Separation of Duties**

ZTA violates separation of duties by dialing down disproportionately on IAM management, leaving other security mechanisms behind.

**Perimeterless**

ZTA is perhaps the only security principle that can reliably secure no-perimeter environments such as WFH

# Zero Trust Basics

1. IAM
2. MFA
3. UEBA
4. Data Segmentation

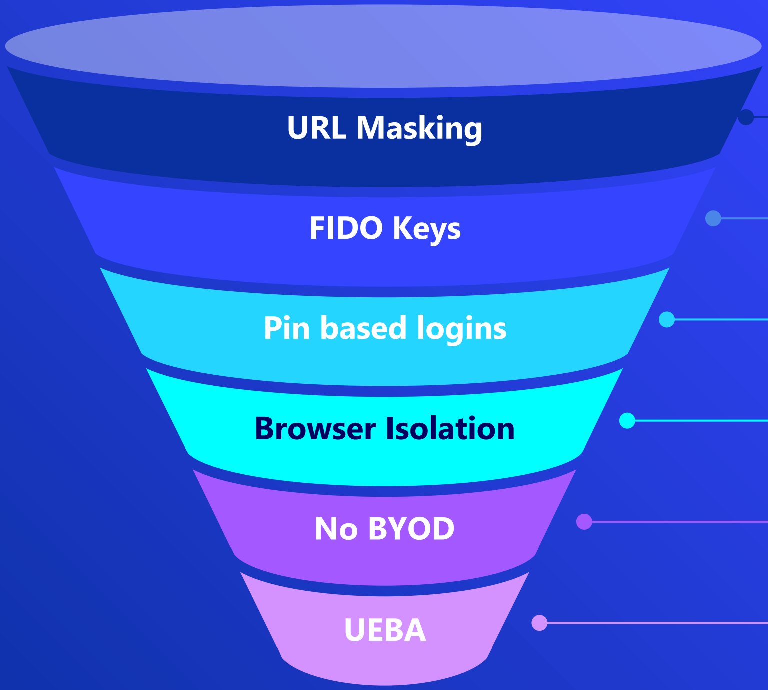
# Solution:

ZTA with all the other principles = Gigantic pyramid of pain!

# Zero Trust Success

1. No Perimeterization
2. Centralized IAM management

# Zero Trust Funnel



**URL Masking**

By masking the URL of all links shared, we can avoid leaking our domains and Ips to adversary.

**FIDO Keys**

FIDO Keys are among the strongest and most reliable forms of Multi Factor Authentication

**Pin based logins**

By removing passwords, we reduce attack surfaces and keep security in place.

**Browser Isolation**

By providing remote browser isolation, website access from custom hardened browsers only, we reduce attack surface

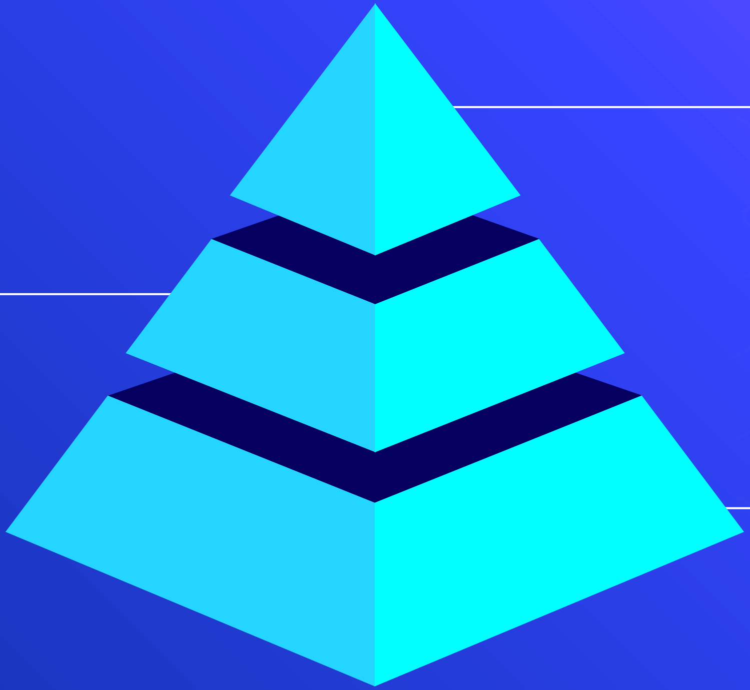
**No BYOD**

By assigning each login to particular company device/s only, we reduce attack surface greatly.

**UEBA**

Utilizing FOSS tools like Elk Stack, Grafana, OSSEC etc for user behavior analysis can harden ZTA

# **Pyramid of Pain:** For the devices on the perimetered network



## Level 1

**Tools, Tactics and Procedures.** By studying the activities of threat actors; we can prepare ourselves according to them, rendering advanced attacks useless

## Level 2

Distinguishing artifacts; i.e. studying network packets for signs of hostile activity. This is usually done **using AI embedded in NGAVs**

## Level 3

Hashes, IP and Domain Blocking; i.e. utilization of typical firewalls and antiviruses