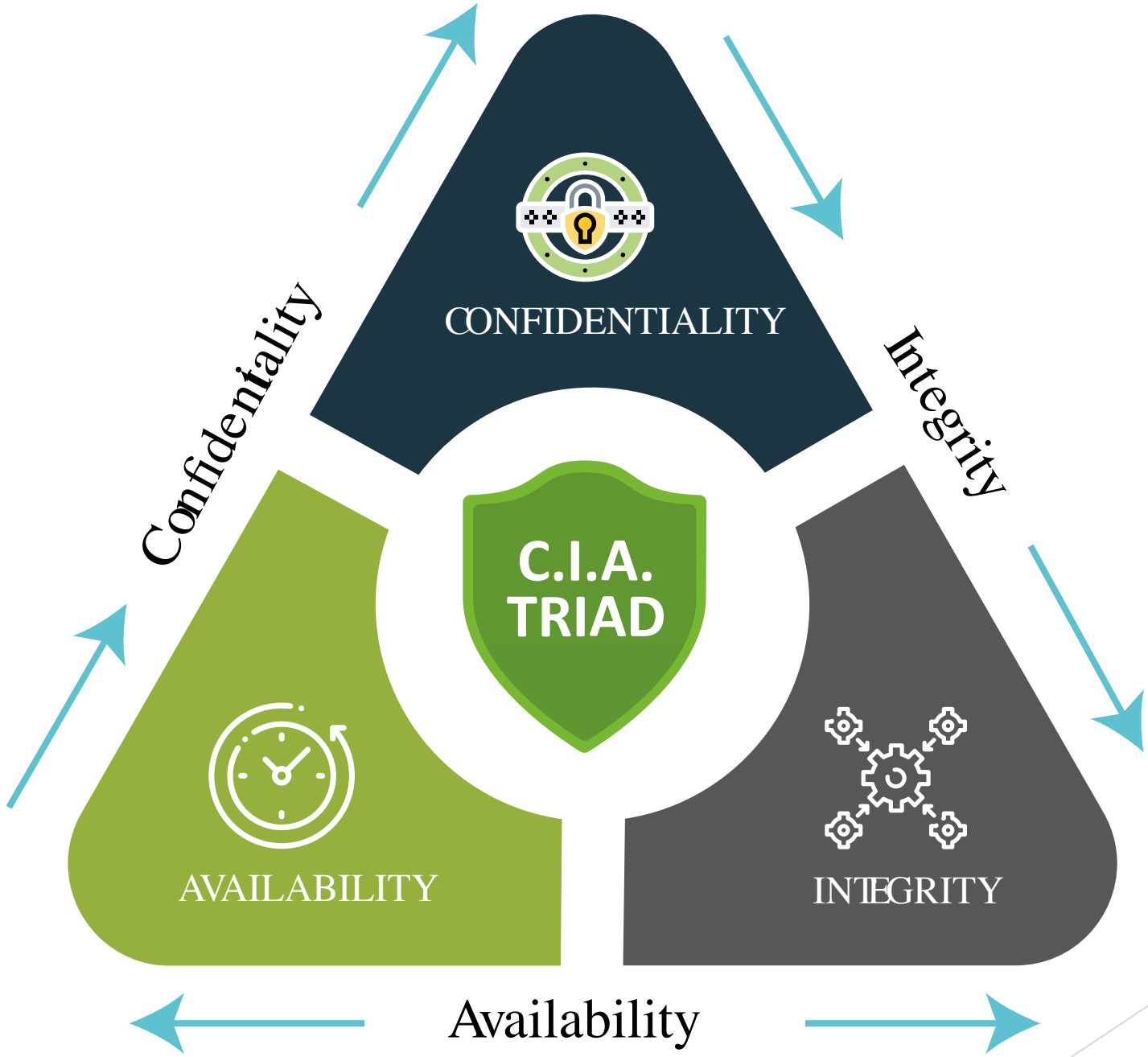
Amazon Web Services
(Security-2)

What is security?

- **Security is the practice of protecting valuable assets.**
  - Assets can be physical or digital and include people, buildings, computers, software application, and data.
  - **Cybersecurity** is concerned with protecting networks, devices, systems, and digital information form the following:
    - Unauthorised access
    - Malicious modifications, theft, or destruction
    - Disruption of intended use
- The primary goal of cybersecurity is to ensure the **C**onfidentiality, **I**ntegrity and **A**vailability of digital information.


Confidentiality
CONFIDENTIALITY
Integrity
C.I.A.
TRIAD
AVAILABILITY
INTEGRITY
Availability

- **C**onfidentiality, **I**ntegrity and **A**vailability - CIA

- **Confidentiality :** is private data protected to prevent unauthorised access?

- **Integrity :** are measures in place to ensure that data has not been tampered with and is correct and authentic?

- **Availability :** Are authorised users able to access the data when they need it?

Basic Security Terms

- **Attacker** : A person or entity with malicious intent to compromise a system
- **Vulnerability** : A weakness in a system that an attacker can exploit
- **Threat** : An event that has the potential to negatively impact a system.
- **Breach** : An attack that compromises a system
- **Control** : A mechanism to reduce or eliminate a vulnerability

Types of threats

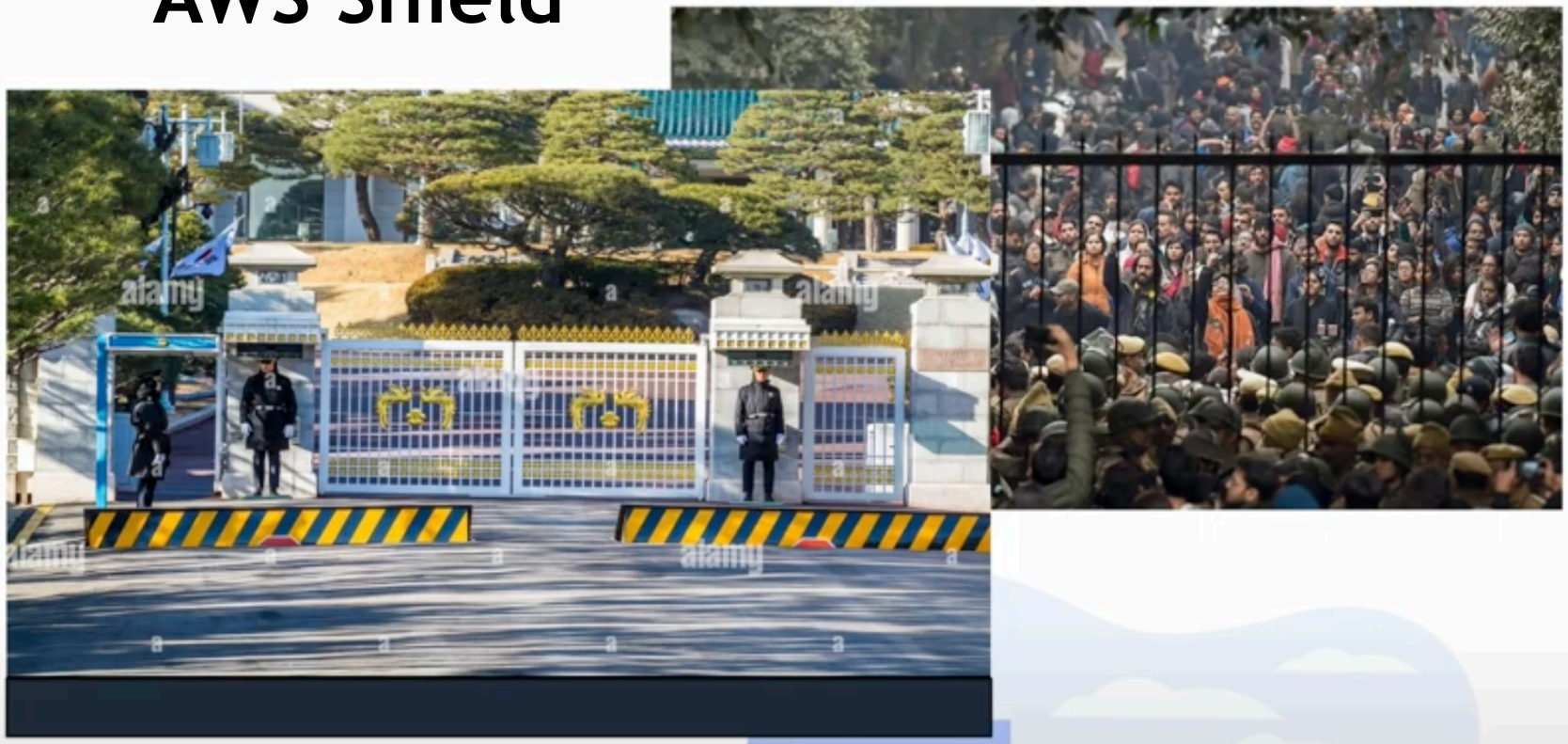
Threat Type	Description	CIA attribute affected
Malware	Malicious software designed to disrupt the operation of a computer system, gain unauthorized access to it, or collect sensitive information from it •Examples: Virus, spyware, worm, remote access Trojan (RAT)	•Confidentiality (virus, spyware, or RAT) •Integrity (virus or RAT) •Availability (virus, worm, or RAT)
Ransomware	Malicious code that restricts access to a computer or its data until a ransom is paid	•Availability
Denial of Service (DoS)	Attack that prevents authorized users from accessing a system	•Availability

Agenda

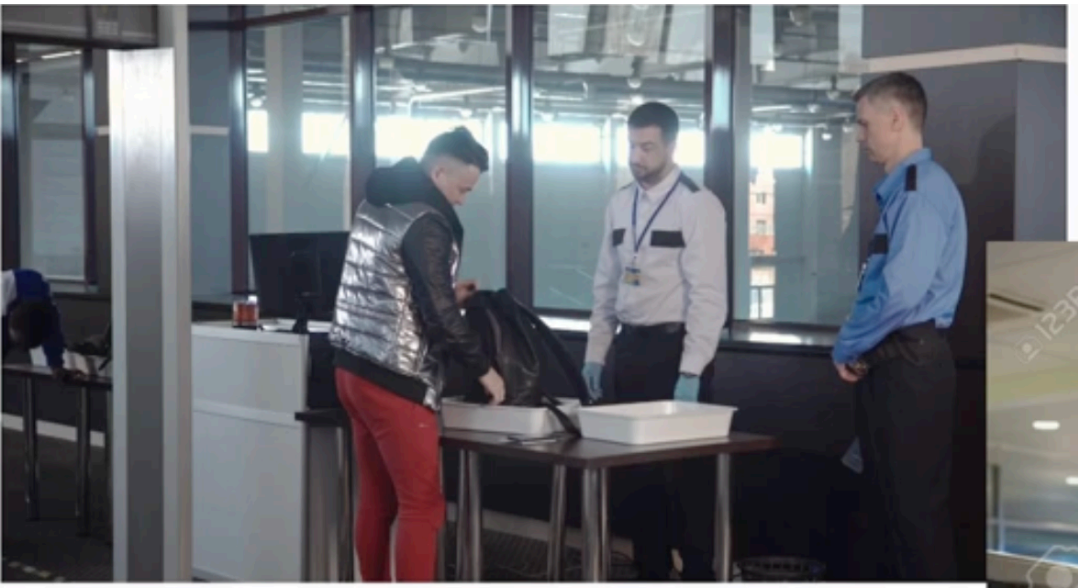
- Shield
- WAF
- GuardDuty
- Inspector

Cloud Infra Security Tools vs House security

AWS Shield



- Shield protects periphery from DDoS attacks.
- Based on the pattern of incoming traffic (big crowd trying to enter, a truck trying to enter the campus), they stop people.
- Shield basically functions at L3/L4 (Transport and Network Layer)



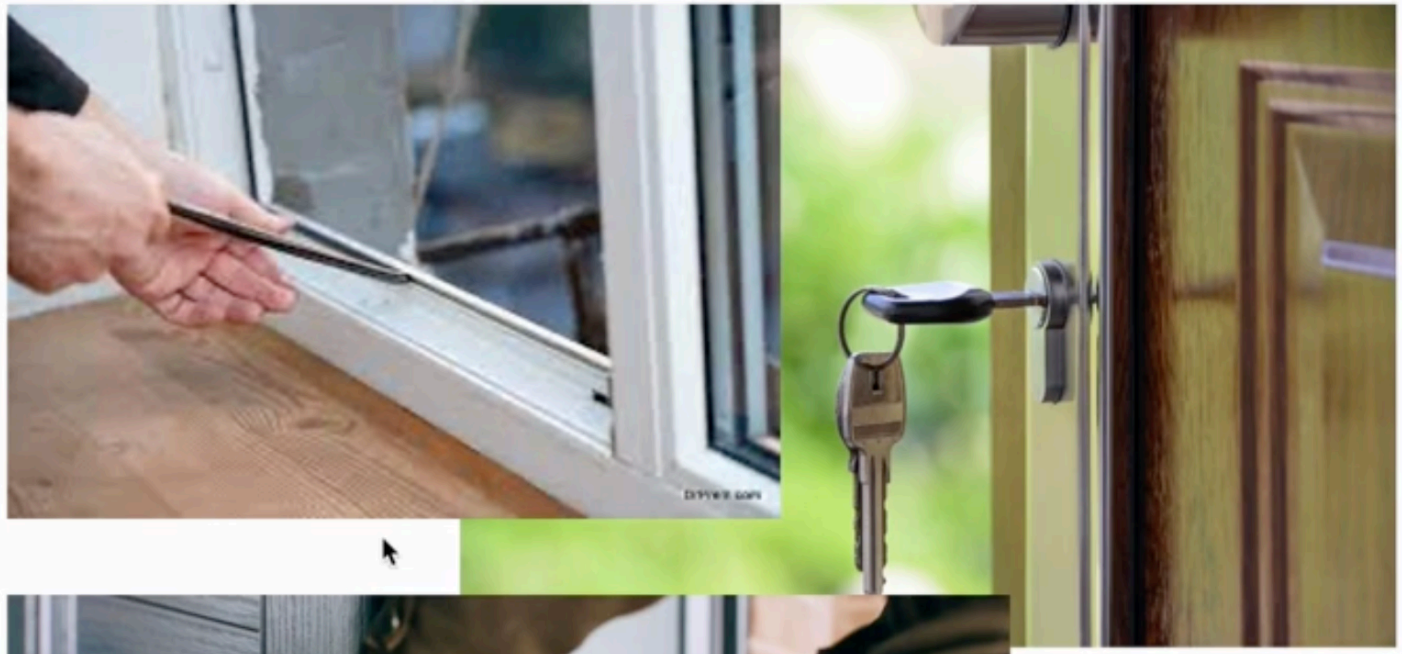
AWS WAF

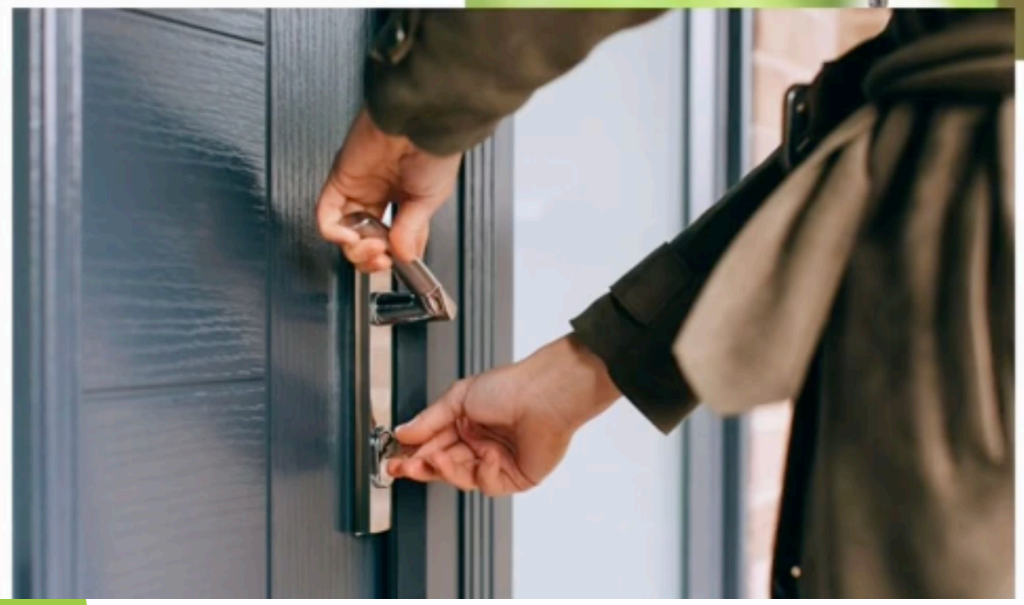
- WAF operates at HTTP layer (L7)
- It can check the origin IP address, http headers etc..
- Similar to security personnel checking your appointment email, checking your bags etc..
- Finally they allow you or block you

Amazon GuardDuty

- GuardDuty keeps analysing the logs (VPC flowlogs, CloudWatch logs, CloudTrail logs etc..) to see if anything suspicious.
- It uses ML/AI
- Intelligence personnel present in the campus will inspect any parcel which is coming in, the food trucks coming in etc. They even check the garbage being put out.
- They don't enter the home!
- They will report anything suspicious.

Amazon Inspector





- Inspector checks the applications running in your EC2 for any security vulnerabilities
- It is like a security person inspecting the windows & doors of the house to see if anything can be broken, breached easily, bullets can pierce through etc..
- Inspector does not operate outside the EC2, but inside!

Feature	AWS Shield	AWS WAF	Amazon GuardDuty	Amazon Inspector
Purpose	DDoS protection for network and transport layers (3&4).	Web application protection from layer 7 (application layer) attack	Threat detection for AWS accounts, workloads, and data.	Automated vulnerability management for EC2, ECR and lambda
Threats Mitigated	DDoS attacks UDP reflection, Floods	SQL injection, XSS, bots, malicious web traffic.	Identifies potential security threats like unauthorised access, anomalous behaviour and compromised credentials	Finds vulnerabilities and misconfigurations in your workloads.
Focus	Ensures service availability during DDoS attacks.	Protects web apps and APIs from malicious HTTP(S) requests.	Monitoring logs and network behaviour for threats.	Scans for software vulnerabilities and compliance issues.
Integration	Works with CloudFront, ALB, Route 53	Works with CloudFront, ALB, API Gateway	Monitors CloudTrail, VPC flow logs, and DNS logs.	Scans EC2 instances, ECR images, and lambda functions.

Summary

- **AWS Shield** : Prevents **DDoS attacks** (availability-focused).
- **AWS WAF**: Protects web applications from **Application-layer attacks.**
- **Amazon GuardDuty** : Detects **suspicious behaviour** and **security threats** in AWS resources.
- **Amazon Inspector**: Focuses on **Vulnerability detection** and **compliance checks** in workloads.