Cloud Security

An end-to-end framework

By: Sibtay Shah

(software dev -> AWS cloud architect -> cloud security)

Meets monthly

discord.defcon908.org

defcon908.org

meetup.com/defcon908

@defcon908

Organizers

Dan Sherry
Organizer
dan@defcon908.org
@netbroom

Jeremy Chisamore
Organizer
jeremy@defcon908.org
@chazb0t

Cid Dominique
Organizer
cid@defcon908.org
/in/cid-dominique-cissp-12326926

Ben Smith
Advisor
ben@defcon908.org
/in/bensmith83

Matt K
Advisor
matt@defcon908.org

Call for Talks

30 minutes + Q&A

- Technical
- Career
- Entrepreneurship or side projects
- “War stories” or research
- Demos
- Workshops

Call for Volunteers

- Admin/resource management
- Sourcing speakers
- Event planning/scheduling
- Handling volunteer meetings
- Website management
- Social media management
- Partnerships with other groups
- Contributing ideas

Introductions

2 minutes each - 15 minutes

Resource Share

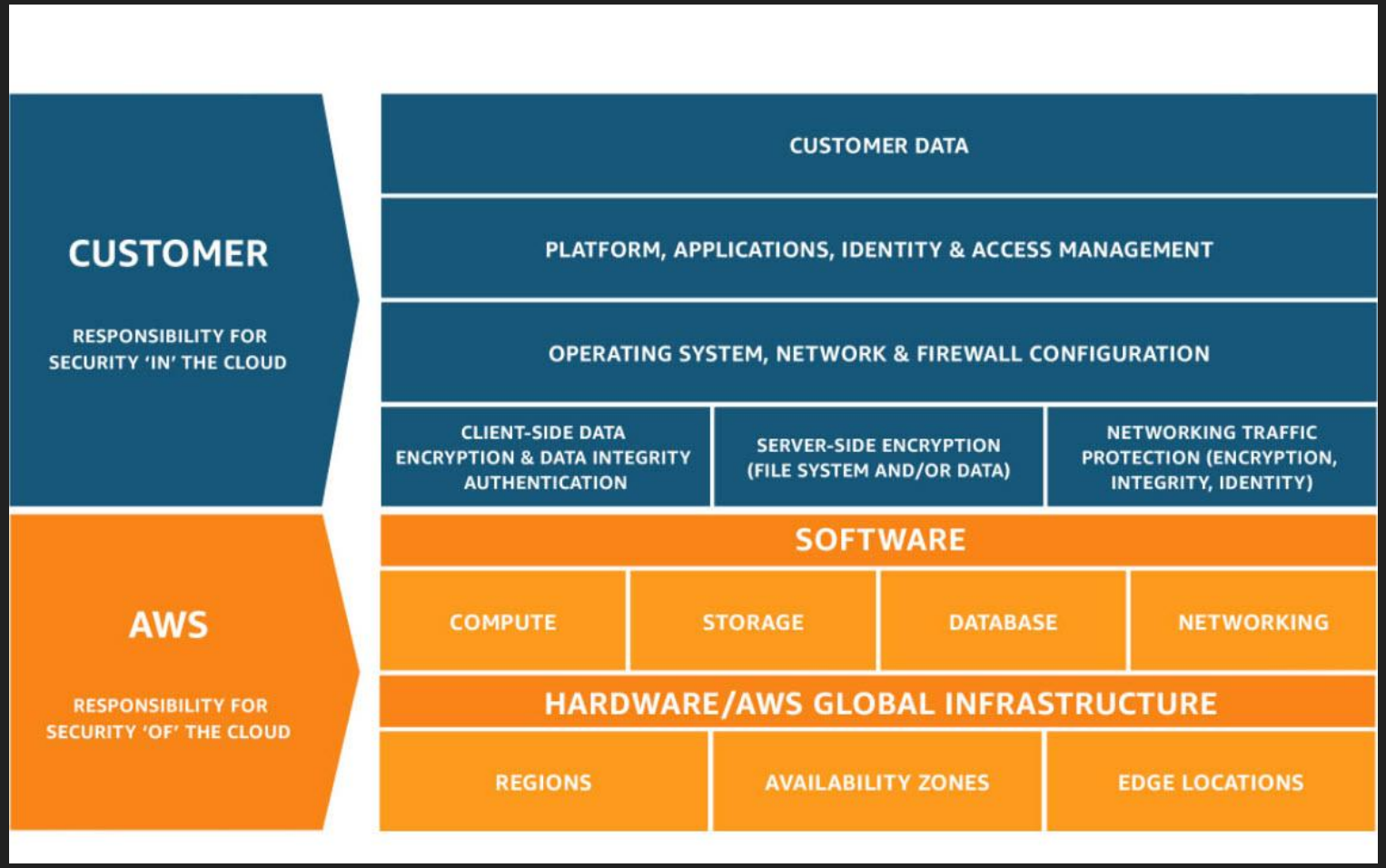
Post to Discord: #resources

Event

Disclaimer: photos may be taken

Cloud Shared Responsibility Model

- Imperative to be aware of your cloud provider's shared responsibility model



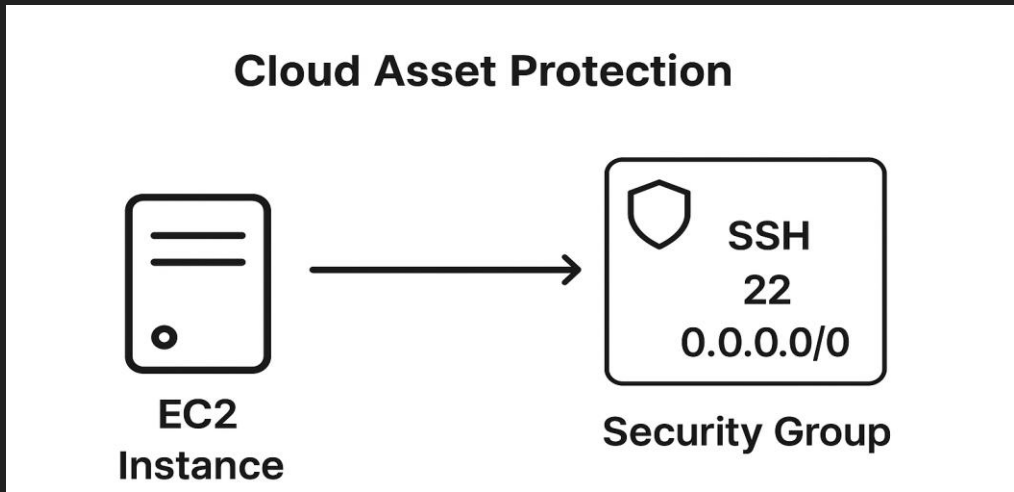
The challenge with securing the cloud

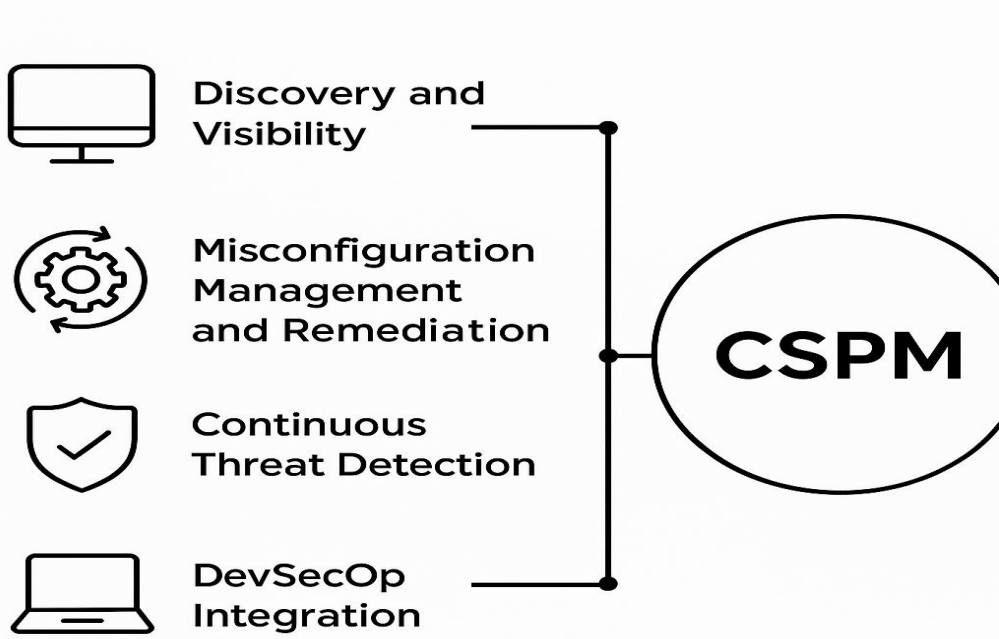
- A large and ever growing list of cloud services
- Dynamic provisioning at scale making **visibility(**inventory tracking**)** and monitoring challenging

Cloud Asset Protection

- Each asset has a configuration that needs to be monitored and hardened

- Enter Cloud Security Posture Management(CSPM)
  - Delivers **visibility, monitoring, and remediation** for cloud assets
  - Continuously **evaluates configurations** against **security best practices** and **compliance standards**



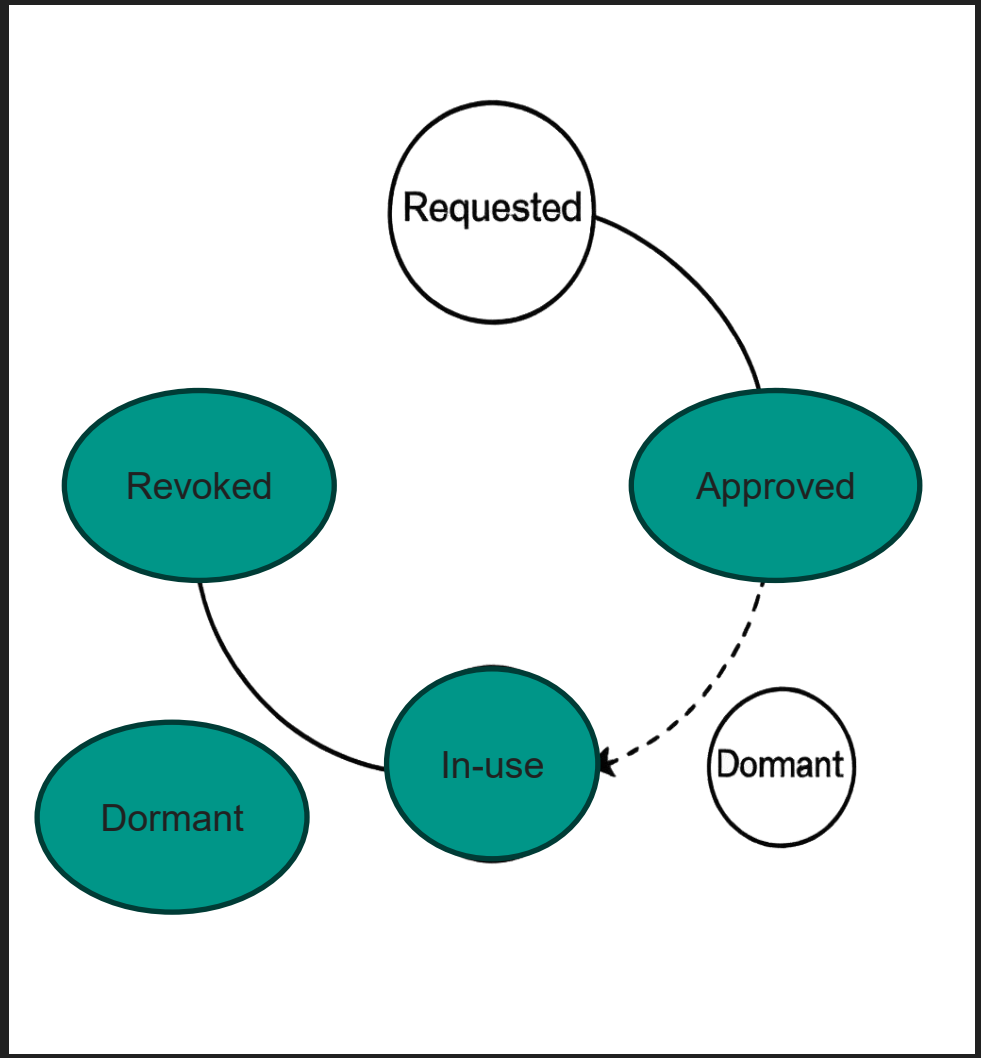


Cloud Asset Protection (..cont)

- For **Kubernetes Cluster** protection we have Kubernetes Security Posture Management (**KSPM**)
  - Same as CSPM but focused on Kubernetes clusters

Identity & Access Management (IAM)

- IAM has a Lifecyle
  - Identity goes through various states (requested ,approved, in-use, dormant, revoked)
  - Access needs change during the life cycle as well (change of job role, change of projects)

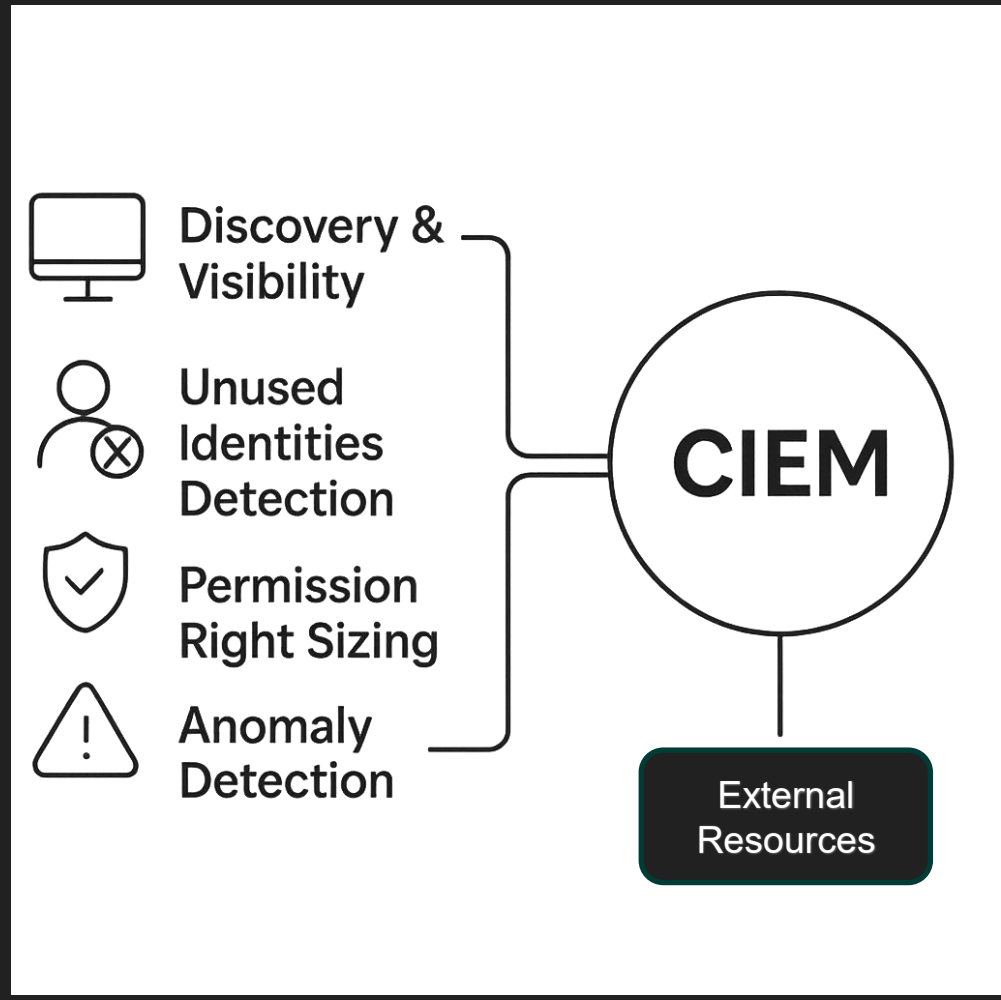


Challenges

- Multiple identity systems
  - **Solution**: Centralized management
    - Identity federation with SSO
    - Helps managing the identity lifecycle but not with access lifecycle management
- Old forgotten identities and privileges
- Excessive/broad privileges
  - Principle of least-privilege (POLP) enforcement

IAM (…cont)

- **Solution**: Cloud Infrastructure Entitlement Management (CIEM)
  - Monitors cloud identities and their permissions
  - Helps enforce:
    - Least privileged permission policies
    - Detection of unused identities
    - Externally and publicly exposed assets (AWS Access Analyzer does)
    - Anomaly detection



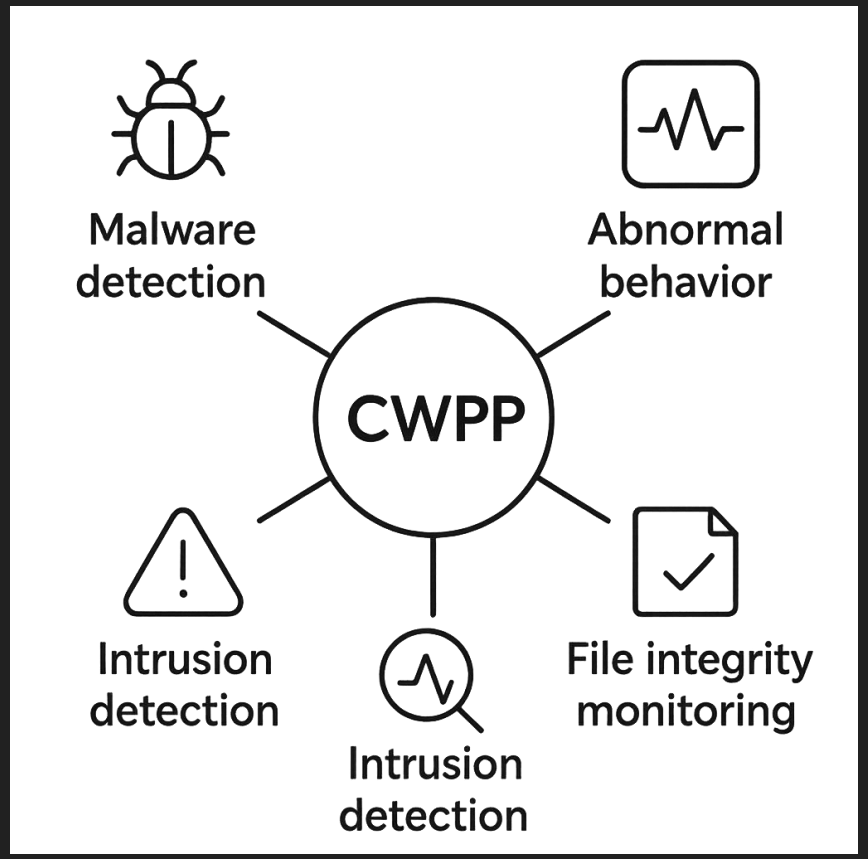
IAM (…cont)

- Secrets management
  - System-to-system authentication
  - Centralized secrets management solutions
  - Secret scanning solutions detects usage of secrets in source code, machines

Runtime Application Security

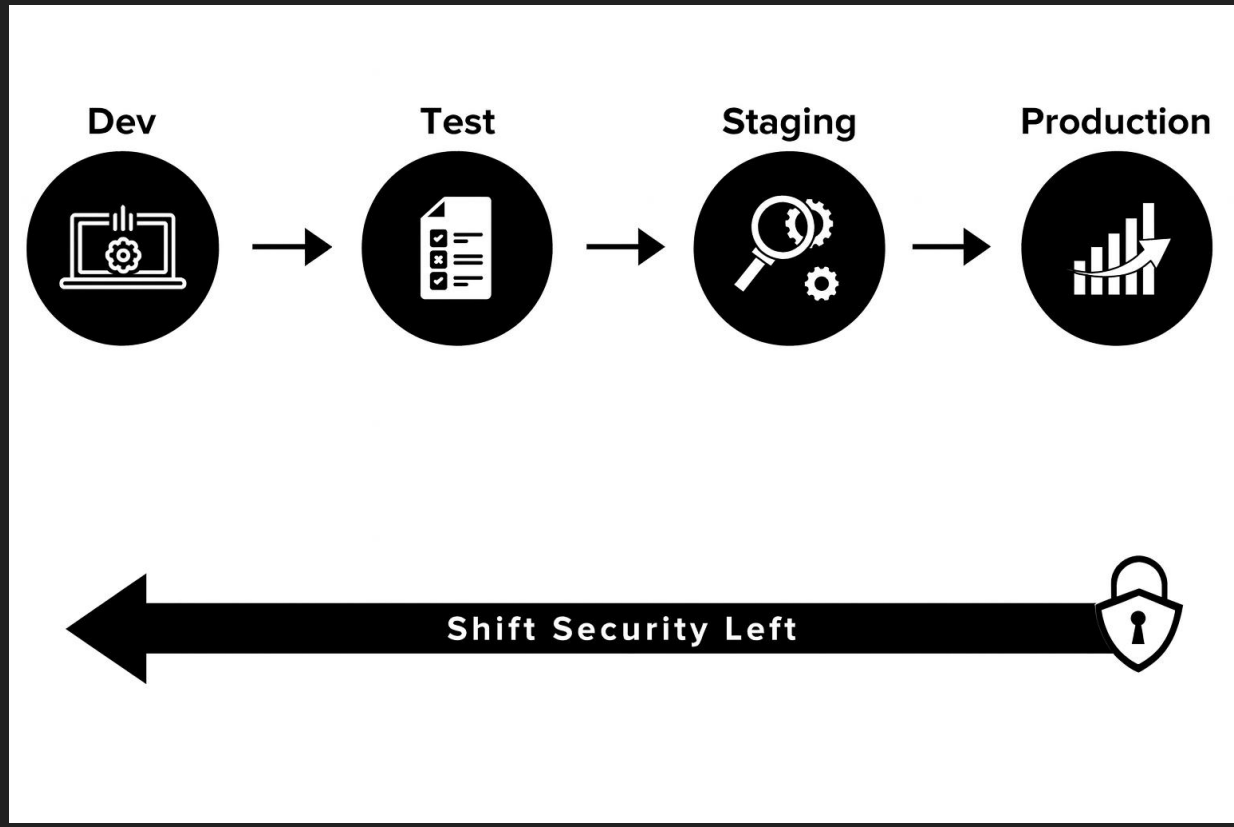
- Runtime protection is needed because:
  - Various undetected vulnerabilities in our system could be exploited
  - Zero-day vulnerabilities

- Enter Cloud Workload Protection (CWP):
  - Continuous monitoring of workloads (servers/VMs/containers) in real time for
    - Malware
    - Abnormal behavior
    - Cryptominers
  - Involves:
    - Intrusion detection
    - File integrity monitoring
    - Vulnerability & Drift awareness with the golden VM/container image



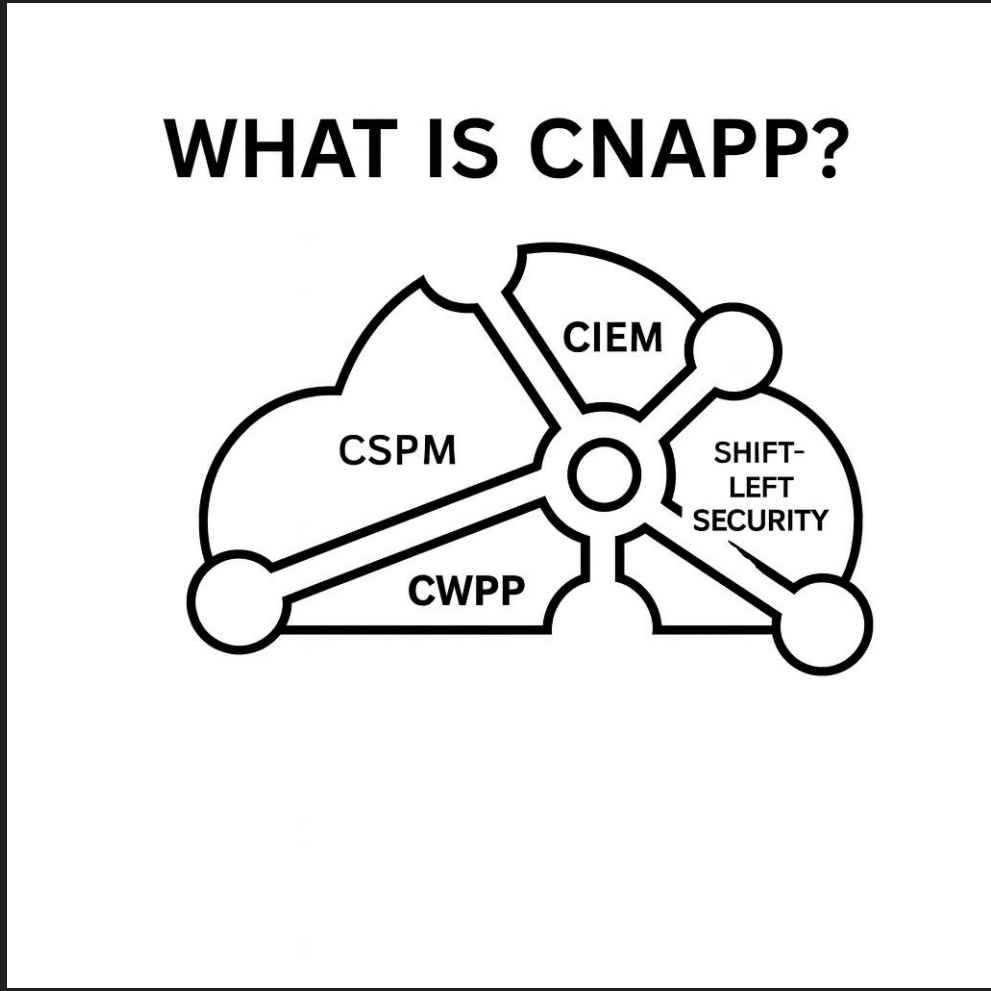
Shift Left Security

- Secure coding practices
- As part of CI/CD pipelines do:
  - Automated SAST and SCA for application and IaC code
  - Secrets scanning
  - Container image scanning before the image gets pushed to the registry
- Security culture in development teams



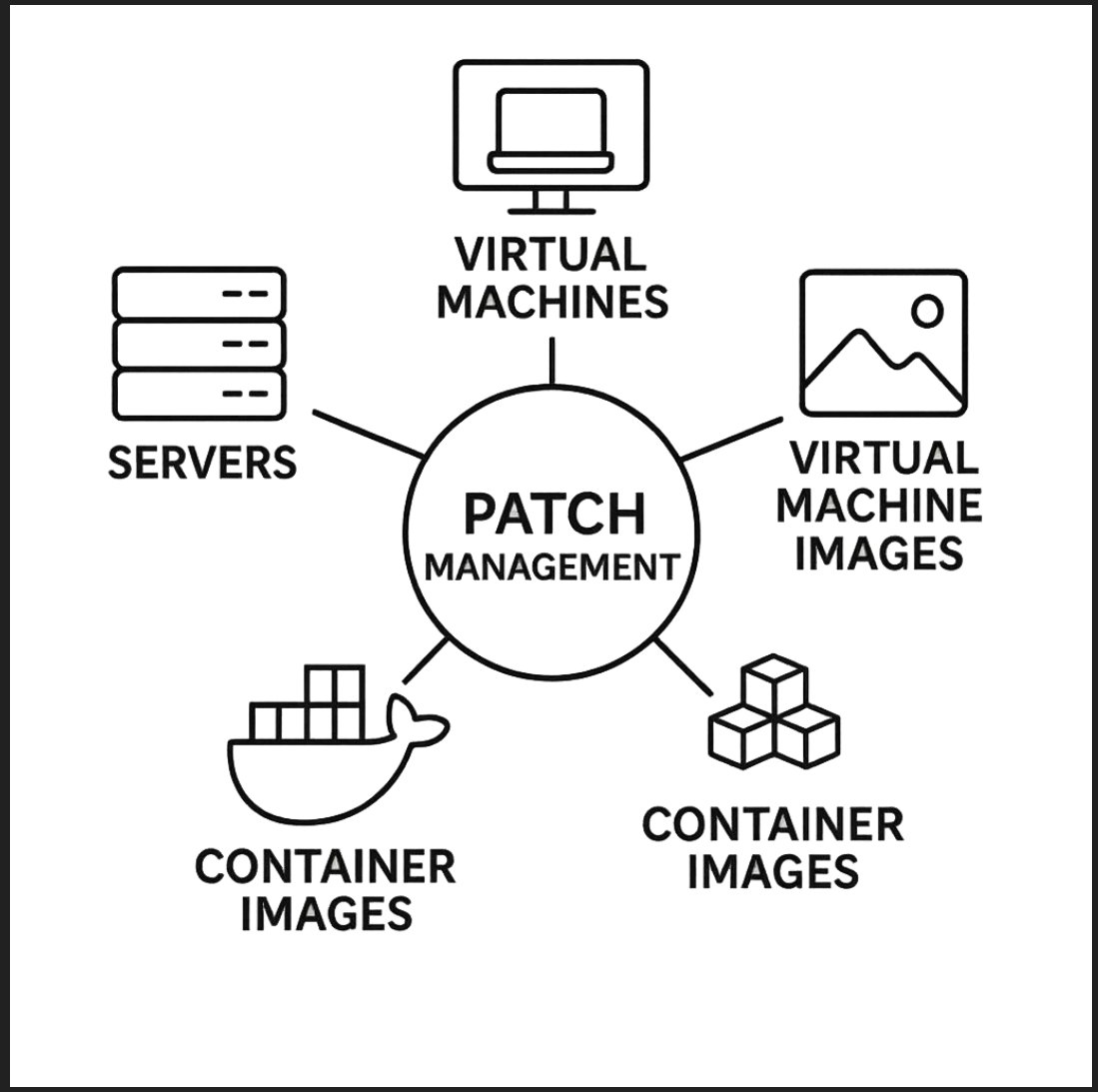
CNAPP (Cloud Native Application Protection Platform)

- A comprehensive security solution designed to protect cloud-native applications and infrastructure throughout their lifecycle, from development to production



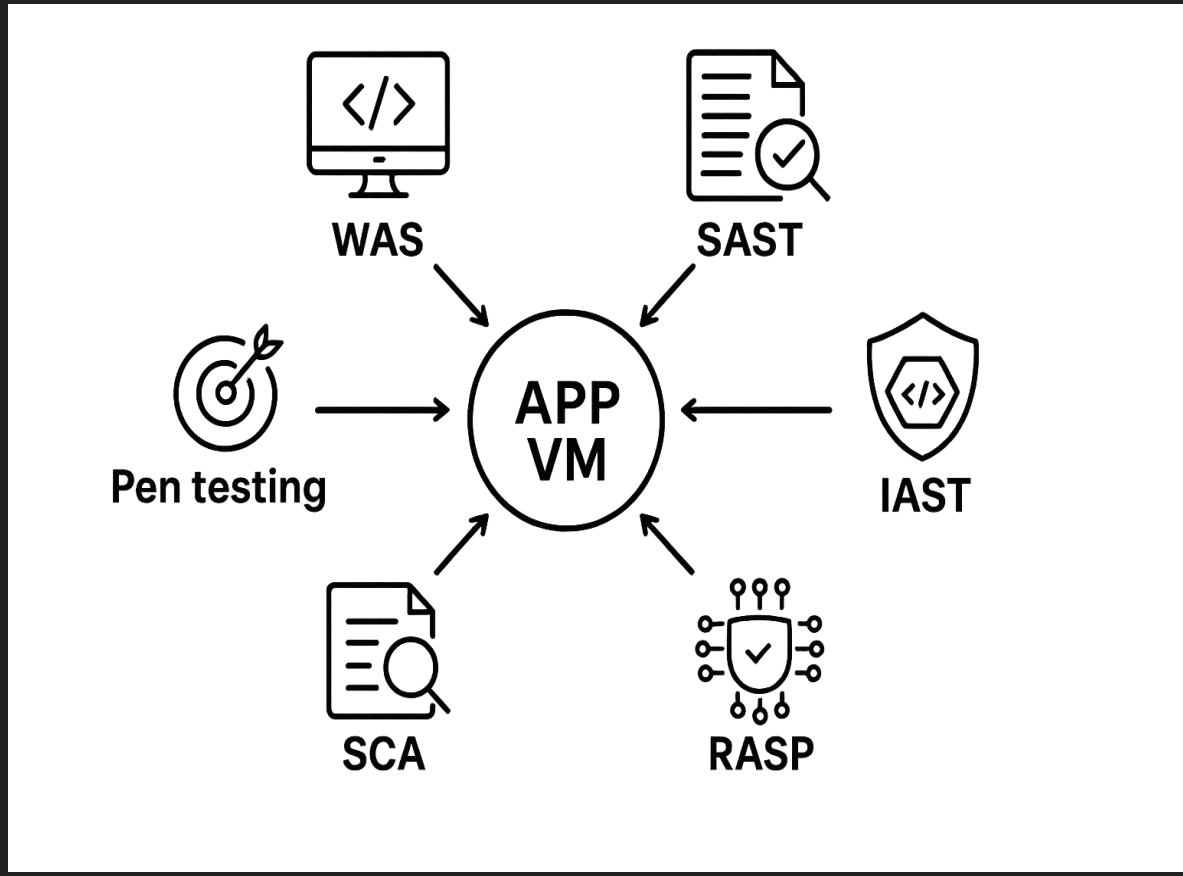
Vulnerability Management (VM)

- Not just patch management
- Patch management is needed for:
  - Servers/Virtual Machines
    - OS & OS packages
    - Agent based/Agentless
  - Virtual machine images (for e.g AMIs)
  - Container images
    - Container image scanning
    - Agents on running container also an option an overkill



Vulnerability Management (..cont)

- Application layer vulnerability management
  - WAS (Web Application Scanning) (*FYI this is an implementation of Dynamic Application Security Testing (DAST)*)
  - SAST(Static Application Security Testing)
  - SCA(Software Composition Analysis)
  - IAST(Interactive Application Security Testing)
  - RASP (Runtime Application Self-Protection)
  - Pen testing
  - CWP(Cloud Workload Protection)



Data Protection

- Data classification
- Tokenization
- Encryption
  - In-transit
  - In-use
  - At-rest

Network Security

- Encryption in-transit
- Firewall (Perimeter control)
  - Virtual Private Cloud
  - NACL rules
  - Security groups (host level firewalls)
- Network Segmentation
  - Subnets: Logical and private/public segregation
- Service endpoint
  - Put as-a-service endpoints virtually inside your perimeter

Network Security (..cont)

- Network defense tools
  - WAF
  - DDoS prevention
  - Intrusion detection and Intrusion prevention systems (IDS/IPS)
  - Egress filtering
  - Data loss prevention