

The ABCs of Cloud Native Security



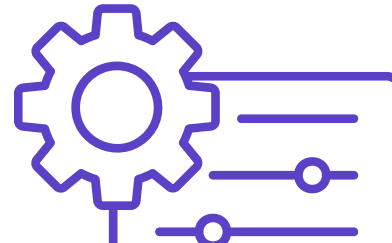
A AI Security Posture Management (AI-SPM)

Secure and verify user identities with robust authentication mechanisms.



B Baseline Configuration

Establish secure configuration standards for infrastructure and workloads.



C Cloud Security Posture Management (CSPM)

Continuously analyze cloud environments to detect misconfigurations, enforce best practices, and ensure regulatory compliance.



D Database Security Posture Management (DPSM)

Monitor and secure database environments by identifying real-time misconfigurations, vulnerabilities, and compliance risks.



E Encryption

Protect data in transit and at rest with strong encryption protocols.



F Firewall Policies

Define granular network access controls to reduce attack surfaces.



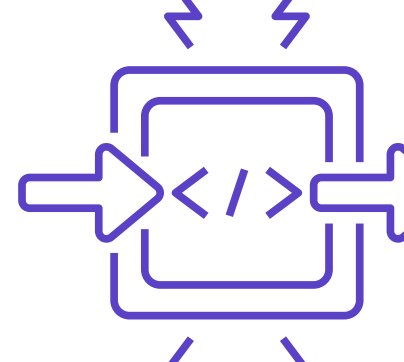
G Governance

Implement policies to ensure compliance and accountability.



H Hardening

Minimize attack vectors by disabling unnecessary features and ports.



I IAM (Identity & Access Management)

Enforce least privilege and tightly control access.



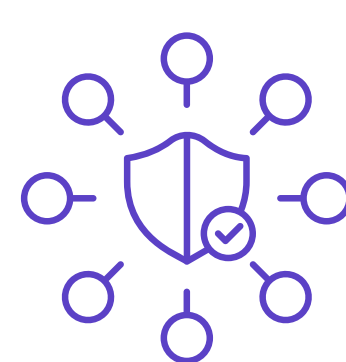
J Just-in-Time Access

Grant temporary access with time-bound permissions.



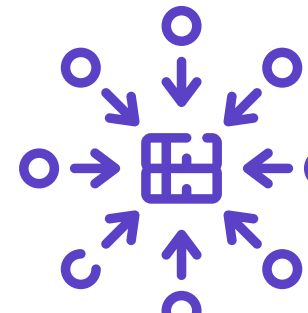
K Kubernetes Security

Secure clusters with RBAC, Pod Security Policies, and network segmentation.



L Logging

Enable centralized logging for auditing and threat detection.



M Monitoring

Continuously observe system behaviour for anomalies.



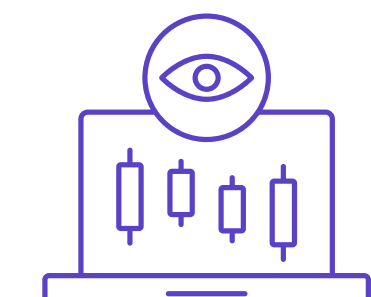
N Network Segmentation

Isolate workloads using service meshes and virtual networks.



O Observability

Ensure full-stack visibility with metrics, traces, and logs.



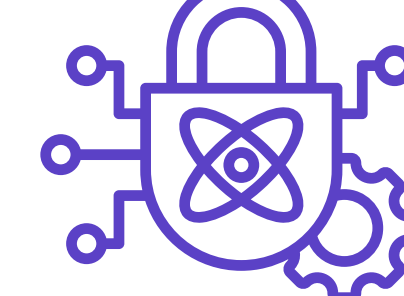
P Penetration Testing

Continuously test and uncover vulnerabilities before attackers do.



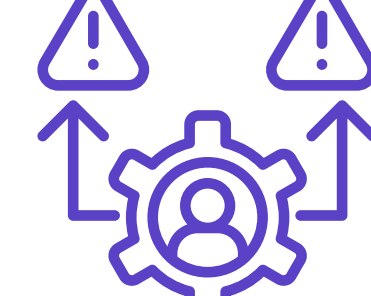
Q Quarantine Strategy

Isolate compromised resources swiftly to contain threats.



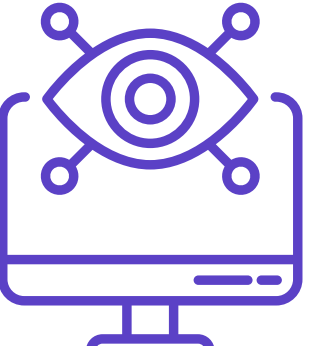
R Risk Advisory

Adapt access controls based on dynamic risk assessments.



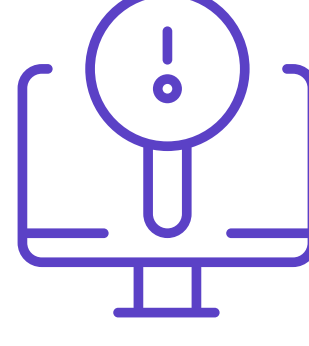
S SIEM & Security Monitoring

Aggregate, monitor, and respond to security events in real time.



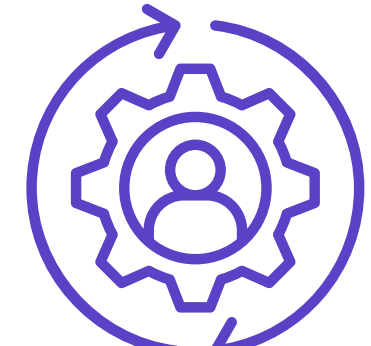
T Threat Detection

Leverage AI/ML to identify and respond to threats proactively.



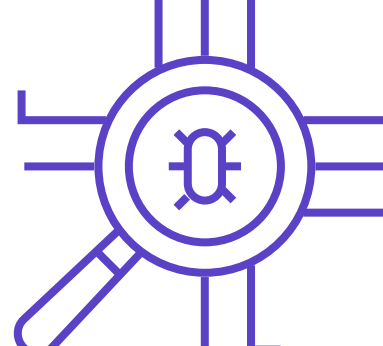
U Update Management

Patch vulnerabilities promptly with automated updates.



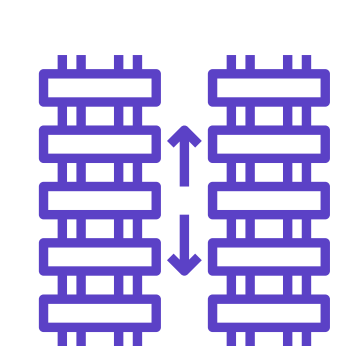
V Vulnerability Scanning

Continuously scan infrastructure and code for flaws.



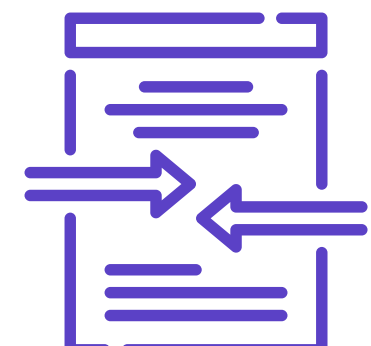
W Workload Isolation

Enforce boundaries between different workloads.



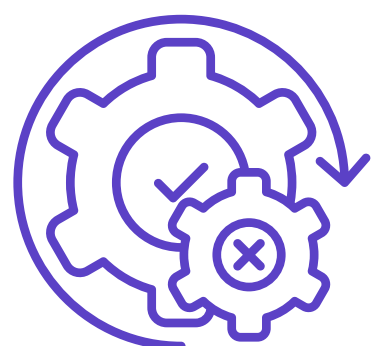
X XML/JSON Validation

Secure APIs by validating all input and output schemas.



Y YAML Hygiene

Avoid misconfigurations in IaC and deployment descriptors.



Z Zero Trust Architecture

Assume breach and verify explicitly for every request.

