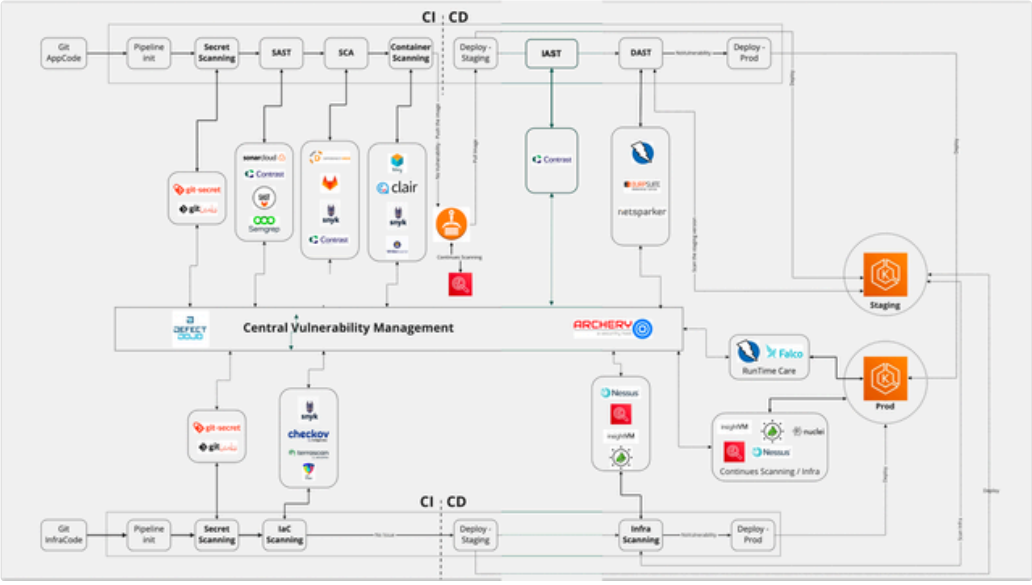
Security Road Map- 2024



Draft Template of the Vision

Infrastructure Security

Security Measure	Description	Examples
Continuous Network and Application Protection (CNAPP)	Ongoing monitoring and evaluation of cloud infrastructure for network and application security.	All-in-one solution to track, alert and monitor security misconfigurations in Cloud Platform.
Cloud Security Posture Management (CSPM)	Check for misconfigurations across the resources and manage them.	S3 bucket being public, IAM Users with Admin access.
Real-time Threat Detection through CloudTrail Events	Continuous monitoring of CloudTrail logs for timely detection / alerting of security threats.	Real-time alerts if MFA is disabled, S3 bucket made public.
Attack Surface Analysis	In-depth analysis of potential attack surfaces within the cloud infrastructure.	Path tracking of attack due to loopholes. IGW → NAT → EC2 port 22.

Identity and Access Management (IAM) Right Sizing - Infrastructure	Right sizing of IAM permissions to ensure the principle of least privilege.	Roles with Admin privileges.
Kubernetes (K8s) Workload Threat Detection	Identification and mitigation of threats within Kubernetes workloads.	Pods with mount to /proc /dev. Processes with sudo access.
On-Prem Server Attack Threat Detection	Implementation of advanced threat detection mechanisms for on-premises servers.	On-Prem server tracking for attacks

Data Security Measures

Security Measure	Description	Examples
Secure Data Acquisition and Handling	Robust processes for acquiring and securely handling data from external vendors. Compliance with data protection regulations and industry standards.	Data download from vendors like up42, Maxar and others.
Encryption and Access Control Framework	Encryption of internally generated data and strict access controls to prevent public access. Logical separation for effective multi-tenancy data isolation.	RDS Encryption, Couchbase Encryption of data at rest and data during transit (TLS).
Data Masking and Anonymization Techniques	Implementation of advanced data masking and anonymization methods. Protection of sensitive information to uphold data privacy.	Handling of PII data during storage and transit.
Comprehensive Data Access Auditing	Logging and auditing of data access activities for accountability. Real-time alerts for anomalous data access patterns.	Data access logs for S3 and detect anomalous IPs / activities.

Code Security Practices

Security Measure	Description	Examples
SAST for CVE Identification	Robust SAST processes for identifying and addressing Common Vulnerabilities and Exposures (CVE). Integration with CI/CD pipelines for seamless code analysis.	Detect XSS, SQL Injection, Code Vulnerabilities
SCA for Licensing and Vulnerability Management	In-depth analysis of software components for license compliance and vulnerability identification. Proactive notification	Open Source License Vulnerabilities(CVE), Policies (LGPL, GPL).

	and remediation for licensing issues.	
Continuous Image Scanning at CI	Consistent scanning of container images for security vulnerabilities. Prevention of insecure images from being deployed into production.	Image Scan Reports before AWS ECR Push / OPA Policies to prevent flagged pulls.
Secrets Detection and Removal	Advanced detection and removal of sensitive information like API keys and credentials in code repositories.	Scan for passwords, secrets, API keys in SCMs.
SBOM Implementation	Generation and maintenance of a Software Bill of Materials for transparent software component management.	Reports of packages used in serving each product.
Real-time Alerts for All New Vulnerabilities	Instantaneous alerts (Day 0) for all identified vulnerabilities globally.	Day 0 notification of new vulnerabilities like log4j and report of usage in repositories.

Network Security

Security Measure	Description	Examples
Application Layer - 7	Attack Vulnerabilities which involves HTTP, FTP, SMTP	SQL Injection, XSS, DDoS Attacks
Presentation Layer - 6	Transactions with Encoding, Encryption	Character Encoding Attacks Enable TLS, SSL
Session Layer - 5	Session Management Attacks	Man-in-the-middle Attacks

Application Security Measures

Security Measure	Description	Examples
IAST Integration	Seamless integration of IAST tools for runtime security testing of applications. Identification and prevention of security vulnerabilities during runtime.	Scan during runtime of applications for security vulnerabilities.
DAST for Real-time Vulnerability Scanning	Dynamic scanning of applications to identify vulnerabilities in real-time. Regular testing of web applications for proactive security measures.	Scan based on inputs during runtime.
VAPT	Scheduled vulnerability assessments and penetration testing for applications. Simulated	Regular VAPT for external sites.

	attacks for the identification and mitigation of security risks.	

Secure Access Management

Security Measure	Description	Examples
JIT Access Provisioning	Implementation of Just-In-Time access provisioning for minimal exposure. Automated provisioning and deprovisioning of access based on predefined user roles.	IAM Access for specified duration and specified permissions. SSH Access with limited permission and limited duration.
Access Reviews and Permissions Management	Periodic reviews of user access rights for continuous security. Identification and removal of unnecessary access permissions.	Regular Access Reviews and reconfiguring roles (SSH and IAM).

Security Operations, Incident Management, and Awareness

Security Measure	Description
Process for Security Risk Management	Clear documentation of processes for identifying, assessing, and mitigating security risks. Incident response workflows and communication plans for efficient incident management.
Continuous Monitoring Solutions	Implementation of continuous monitoring solutions for real-time threat detection. Proactive response mechanisms to security incidents.
Stakeholder Awareness Programs	Regular training programs and awareness campaigns for all stakeholders. Fostering a culture of security awareness throughout the organization.

Tools to be considered

- SCA: FossID, Fossa, BlackDuck, JFrog
- CNAPP: Tenable, Cloudanix, PingSafe
- SAST: SonarCloud
- AWS Native: AWS Detective, AWS Security Hub, AWS Config, AWS Inspector

- **AWS Detective**:
  - **Azure Sentinel**: Azure Sentinel is a scalable, cloud-native solution for security information event management (SIEM) and security orchestration automated response (SOAR).
- **AWS Security Hub**:
  - **Azure Security Center**: Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
- **AWS Config**:
  - **Azure Policy and Azure Resource Graph**: Azure Policy helps enforce organizational standards and assess compliance at-scale. Azure Resource Graph allows you to query resources and explore their relationships.

- **AWS Inspector**:
  - **Azure Security Center and Microsoft Defender for Cloud**: Azure Security Center, in combination with Microsoft Defender for Cloud, provides advanced threat protection for workloads running in Azure and other environments. This includes vulnerability assessments, similar to AWS Inspector.