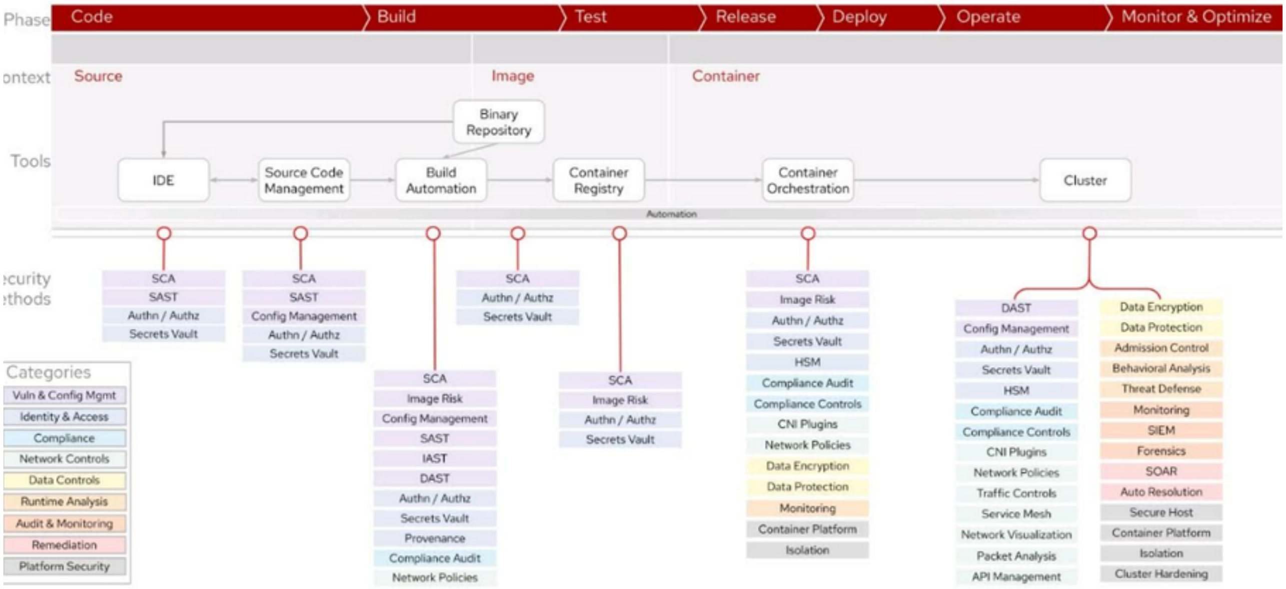
Security: DevSecOps Roadmap

📋 Overview

To define the security practices as well as Identify & remediate the security gaps in DATA pipeline across LDT to improve the product security posture

DevSecOps Flow Diagram



	Goal	Requirements	Status
1	☑ **Static Application Security Testing (SAST)** - Lentra SonarQube	- Scans source code for Bugs, vulnerabilities, and Code smells. - Quality gate - Integrate with CI pipeline	DONE
2	☑ **Software Composition Analysis (SCA)** Software composition analysis (SCA) is an automated process that identifies the open source software in a codebase i.e. to analyze code security and quality	Analyze code security as per, - Package managers - Manifest files - Source code - Binary files - Container images - Generate Software Bill of Material (SBOM) for known and common vulnerabilities	DONE

3	☑ **Automate pipeline to Identify secrets & credentials from the code**	• Identify Secrets/Credentials/Token/Keys from the codebase to prevent data breach	DONE
4	**Insufficient logging and monitoring**	• Audit trail for logins, failed logins and sensitive transactions • Real-time attack alerting • Robust and consumable logs • Incident response and recovery plan [TBP]	
5	☑ **Identify vulnerabilities from application container images**	• Identify vulnerabilities from application container images	DONE
6	**Vulnerability Management Platform**	• Manage application security program, • Maintain product and application information • Triage vulnerabilities • Push findings to systems like JIRA and Slack	
7	**Compliance as code**	• Create Inspec profile to create compliance checks • Continuous compliance in pipeline	
8	☑ **Infrastructure as Code (IaC)**	• Scan infrastructure as code for misconfigurations • Detect security vulnerabilities and compliance violations • Security and compliance best practices for AWS, Azure • Detects AWS credentials & Identifies secrets • Mitigate risks before provisioning cloud native infrastructure.	DONE
9	**Implement Risk Management Framework**		
10	☑ **Secure Data Pipeline in AWS**	**Logging and Monitoring:** • All of the AWS Data Pipeline actions are logged by CloudTrail	DONE
11		**Data encryption:** • Encryption of data at rest ◦ Amazon S3-managed server-side encryption keys (SSE-S3) with AWS KMS ◦ Encrypt the metadata stored in the AWS Glue Data Catalog and the logs generated by AWS Glue crawlers and ETL jobs using AWS KMS • Encrypting Data Catalog ◦ Encryption of AWS Glue Data Catalog objects which include the following: ▪ Databases	

		▪ Tables ▪ Partitions ▪ Table versions ▪ Connections ▪ User-defined functions • Encryption of data in transit ○ Transport Layer Security (TLS) encryption for data in motion between AWS Glue and S3	
12	**Container Security**		
13	**API Security**		