

Secure Software Development Lifecycle™

Point of View

March 2023

Table of contents

- 1 Service offering overview**
- 2 Customer challenges on securing dynamic cloud environment**
- 3 Secure the modernized environment with Deloitte's SSDL**
- 4 The approach for deploying SSDL**
- 5 Appendix**
- 6 Demonstration**



Service offering overview: SSDL model

Service description

SSDL is a modular orchestration platform capability designed to help organizations develop use cases based on cloud security and compliance requirements. Deloitte leverages this capability to help clients address requirements from design strategy to tactical build/deploy and finally manage observability through assessments. SSDL leverages base solutions from Deloitte alliance vendor Palo Alto, proprietary custom code, and integrated workflows to help clients address their requirements. The capability can be integrated as part of the overall solution or within an existing client's cloud security and compliance solution ecosystem. SSDL can scale across multi-cloud platforms. SSDL leverages Palo Alto's technology stack to establish a mature cloud security program that can help clients address end-to-end security requirements at each stage. The SSDL capability is designed to help safeguard clients' cloud environments by standardizing account provisioning, enabling secure build and deployment, logging and monitoring, and enforcing custom guardrails.

Market Channels: Direct to market | Alliance channel

Market Offerings: Cyber: Strategy, Implement, Operate | Integrate with CI/CD (continuous integration and continuous deployment)for Multi-cloud Tool | Integrate with DevSecOps Offering

Key Identifiers

- Continuous compliance and security monitoring across multiple domains
- Network and infrastructure;
- Data and encryption;
- IAM security; and
- Logging and monitoring
- Technical security baseline translation from organizational Security requirements
- Reduced threats to multi-cloud eco-system
- Security from early stages and speedy recovery from mis-configurations/policy deviations
- Improved agility and feedback loops
- continuous operational support to reduce alert fatigue

Offering Outcomes

- Standardized account vending processes
- Standardized enablement of security guardrails across all phases of development lifecycle
- Misconfigurations fixed early in the development lifecycle
- Visibility across all cloud environments, phases, and workloads with a single pane of glass view
- Near real-time remediation for misconfigured alerts with fine grain exception control
- Close alignment to organization approved exceptions and change management
- Reduced alert fatigue for the SOC analysts

Tools and Accelerators

- Policy as Code (PaC) guardrails repository to detect, prevent and remediate mis-configurations in each phase of the DevOps pipeline
- Automated PaC installation and technical guides
- Security automation architecture patterns for cloud accounts and workloads
- Technical configuration and code libraries of automation scripts for Industry specific use cases
- Custom orchestration workflow playbooks for Security automation and orchestration
- Continuous reporting and visualization with real-time dashboards
- Correlation searches for advanced user analytics and behavior detection

Service offering owner

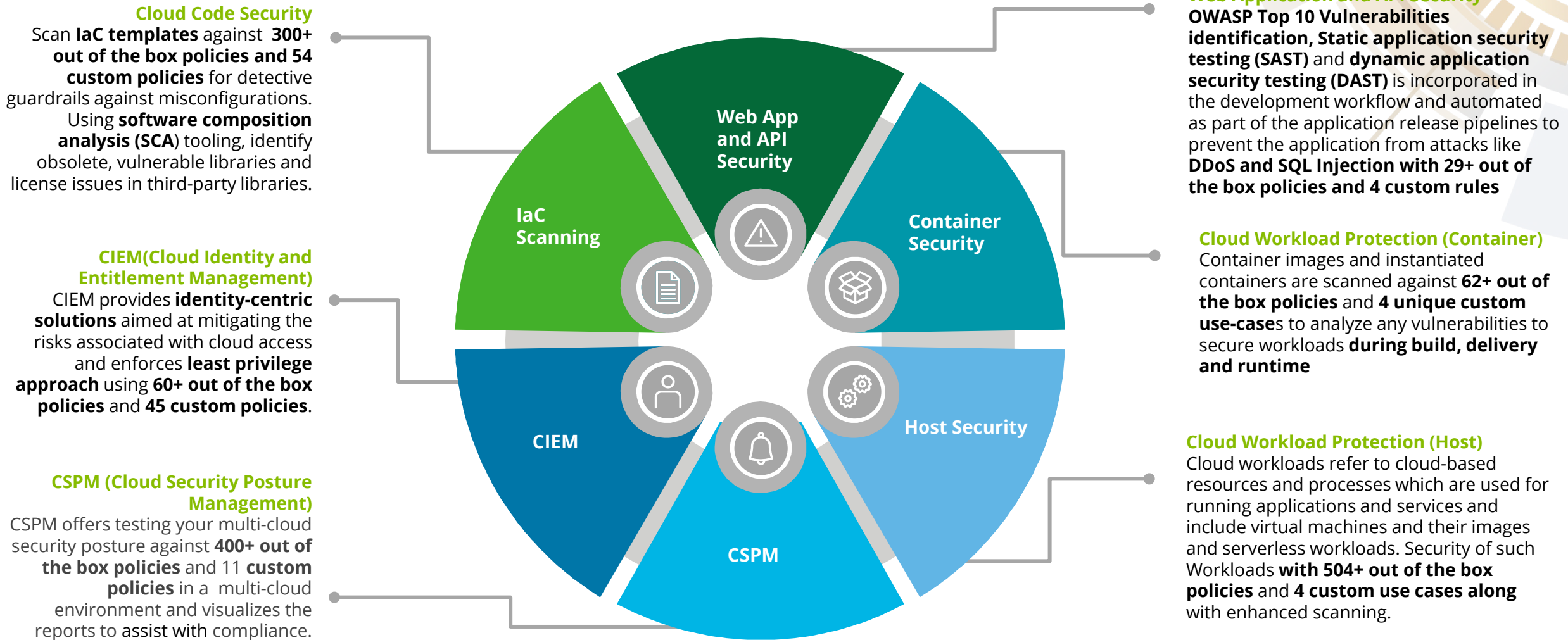
Kieran Norton and Jane Chung

Service offering lead

Sid Kantroo

SSDL footprint

Visibility of SSDL's coverage for below domain offering



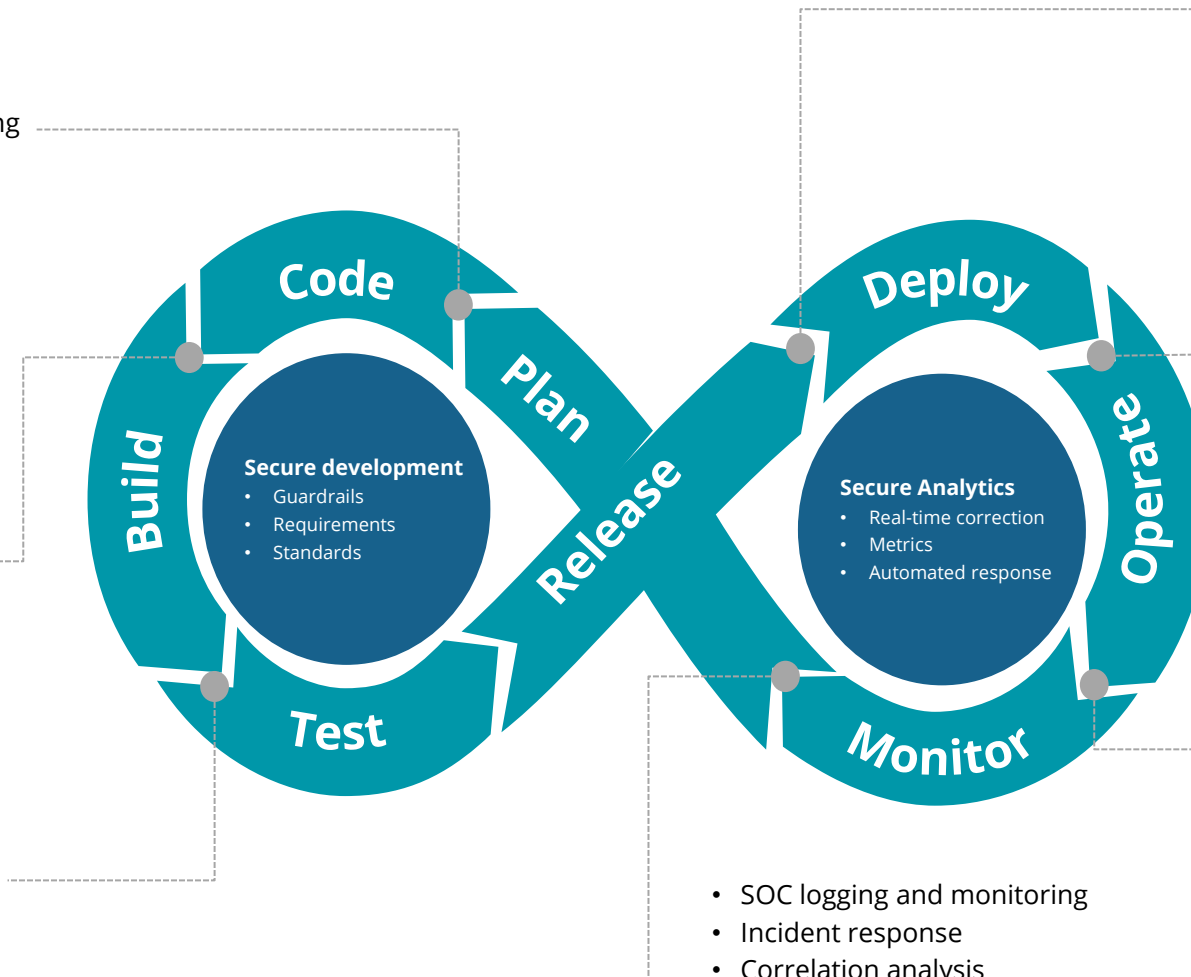
How can SSDL help 'secure at every phase'?

In the SSDL model, security controls are continuously integrated into the development, deployment, and operations stages

- IDE, VCS security scanning plugins
- Infrastructure as code scanning
- Open API, ARM, serverless template scanning
- Policy as Code
- Early VM and compliance feedback in developer integrated development environment (IDE) or CLI tooling

- CI/CD pipeline scanning plugins
- Container image scanning
- Supply chain Security
- Secrets scanning
- Software composition analysis
- Infrastructure security testing
- Vulnerability management and compliance with industry standards
- Collaborative guardrails injected with static code analysis early into development process

- Dynamic application security testing
- Image analysis sandbox
- Trusted images validation
- Enforce security policies automatically and perform automated attacks against pre-production code



- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWP)
- Web Application and API Security (WAAS)
- Cloud Infrastructure Entitlement Management (CIEM)
- Prevent pre-production code from reaching production if cloud configuration scans doesn't pass automated compliance scans

- Secure greenfield environment
- Deloitte automation with runtime alert remediation
- Threat detection, network security and data security
- Insights into all cloud resources and changes. Automatically remediate misconfigurations to secure state

- Deloitte automation to handle drifts
- Centralized logging architecture in cloud
- Palo Alto Networks Prisma® Cloud logs export to SIEM/XDR tool
- Log ingestion to Palo Alto Networks Cortex XSOAR tool for incident response
- Log health and security relevant events. Near real-time threat and user behavior protection

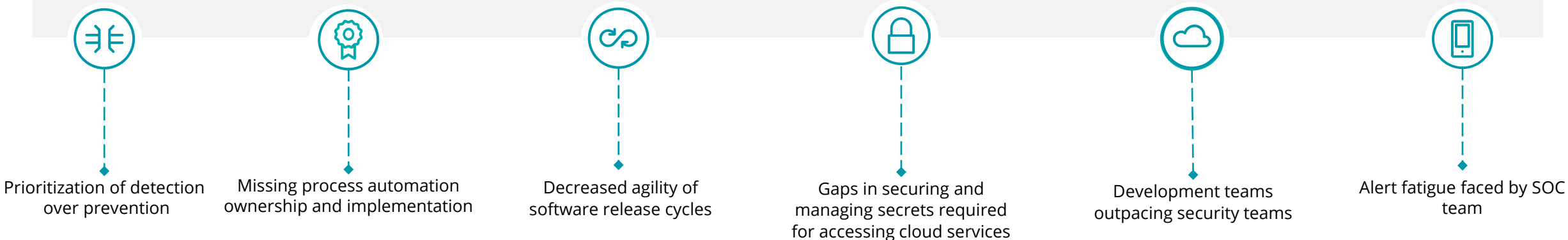
- SOC logging and monitoring
- Incident response
- Correlation analysis
- Monitor the production environment for deviations from expected behavior and exploitation of known/unknown vulnerabilities

Common customer challenges with securing a dynamic cloud environment



Software development lifecycle challenges

Businesses are prioritizing becoming more agile, reducing cost, and simplifying information technology (IT) with cloud and disrupting traditional infrastructure, application technologies, and environments. These transformational changes are driving the need for organizations to adopt a different approach to cloud security to keep pace with cloud adoption, DevOps scale, automation, and an evolving cloud attack surface.



Secure the modernized environment with Deloitte's SSDL



SSDL overview

In the era of digital rapid transformation and disruption, the need to accelerate the implementation of secure deployment of infrastructure has become important; to help organizations address this, the SSDL introduces the concept of security in every phase of DevOps Lifecycle

Transformation to SSDL

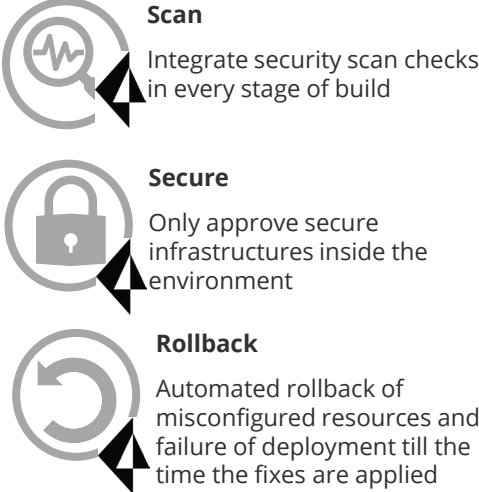
Moving to an SSDL model is both a strategic and continual improvement process aimed at delivering continuous security, increased efficiency and product quality, enhanced compliance with industry standards (PCI,HIPPA,CIS), increased collaboration and reduced costs. It follows the approach of implementing security at every stage of development lifecycle along with continuous feedback to the previous stage that enables the enhancement of security guardrails and enforces implementation of configured resources.



Scan | Insightful | Detective | Review/Refine

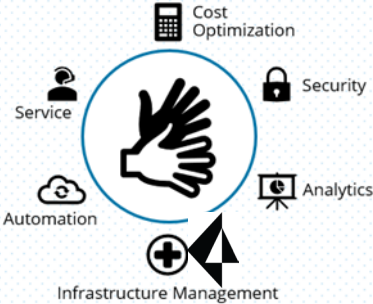


Preventative | Secure deployments | Rollbacks



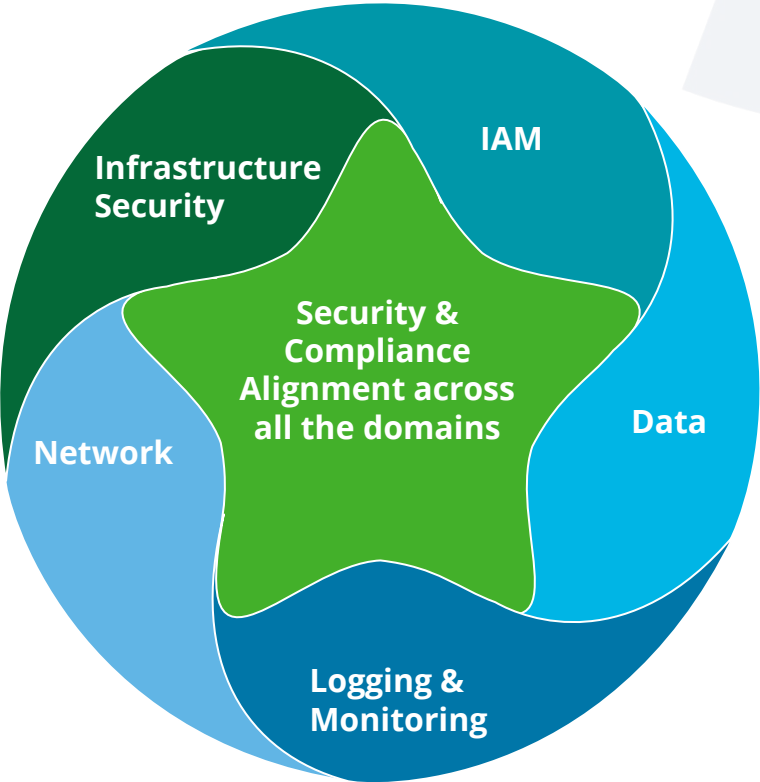
Monitor | Corrective | Alert

Continuously monitor the configurations of the infrastructure for compliance, technical or baseline control drifts, auto correct misconfiguration in real time and implement advanced threat detection use cases on SIEM and SOAR



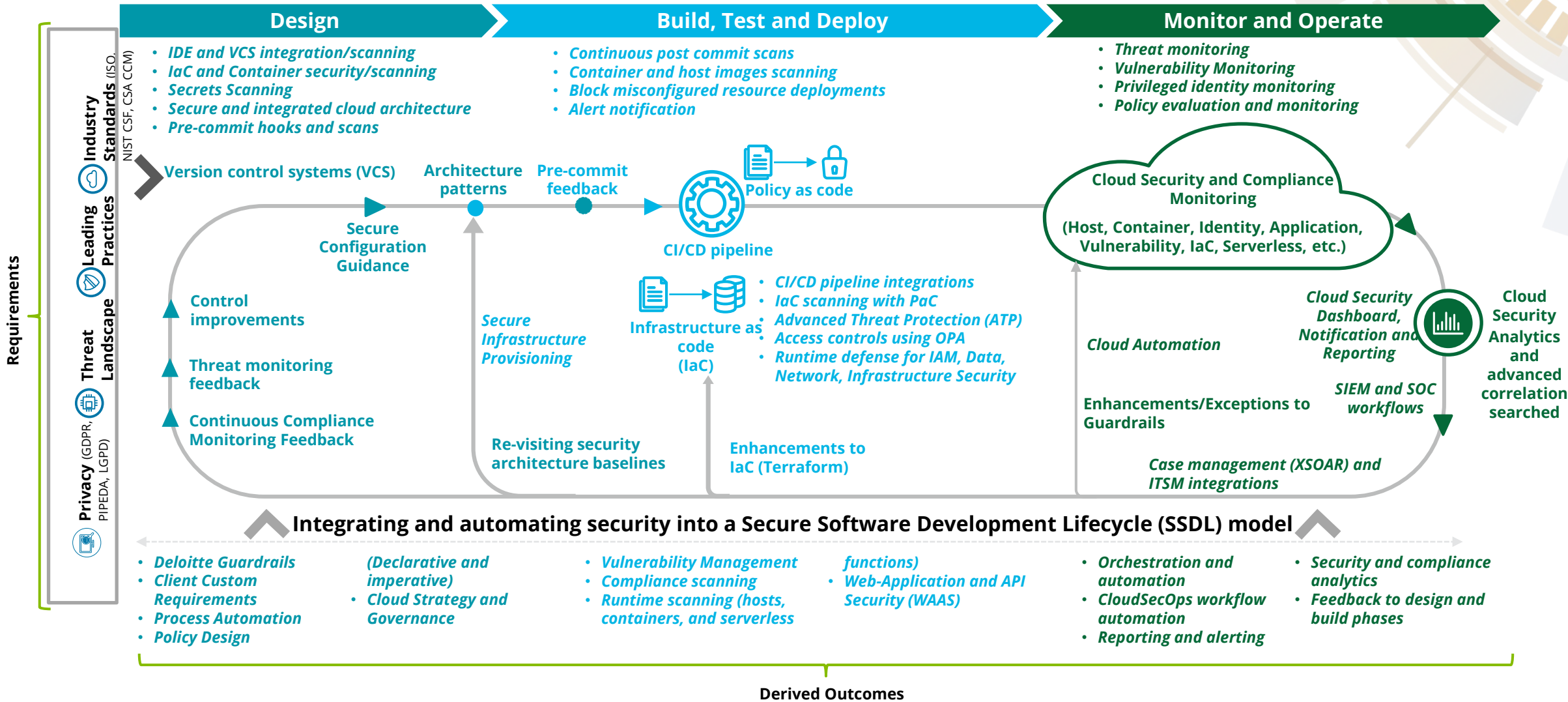
Cyber Capabilities

SSDL provides secure and reliable development lifecycle across security domains to help you align to industry leading compliance frameworks.

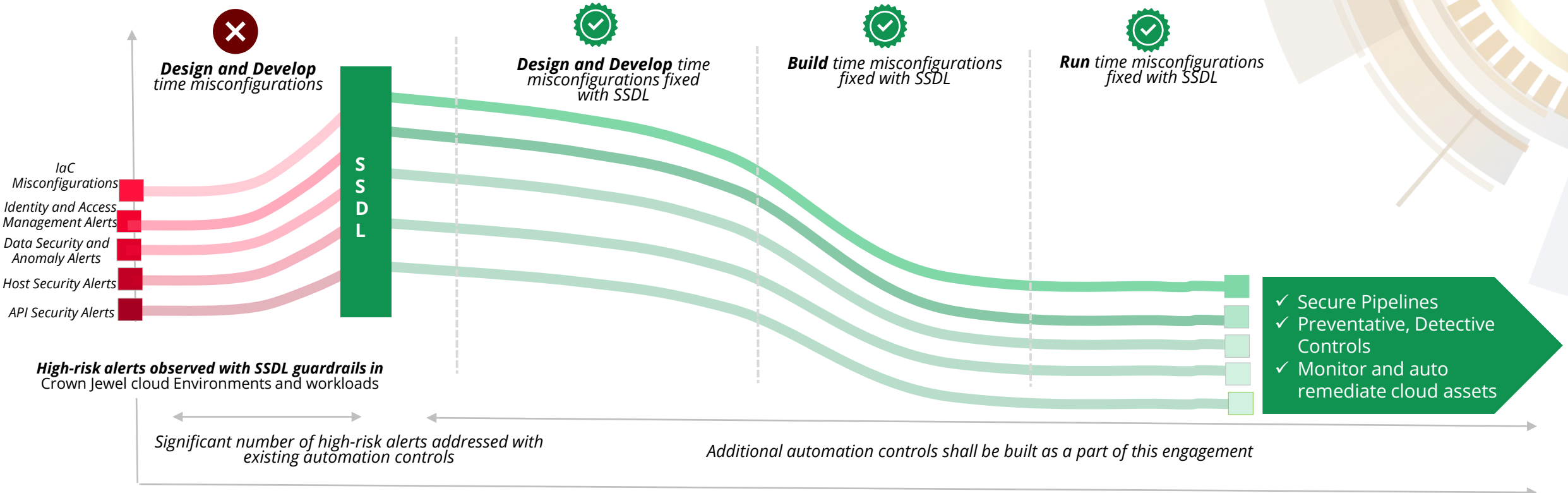


Transition into SSDL model

Organizations should consider integrating and embedding security in each step of their cloud journey, to safeguard their cloud environment and develop the ability to proactively react to adverse cyber incidents. Diagram below illustrates how SSDL model can integrate security capabilities at each step.



Value of SSDL



Without SSDL With SSDL

Without SSDL	With SSDL
<p>Minimum effort required can be ~10,000+ effort hours</p>	<p>Leveraging SSDL (Palo Alto Networks + Deloitte Automation) can provide ~ 50% savings* (~5000 hours in reduced effort)</p>


* Actual savings will vary based on individual cloud ecosystem and their configurations

Scenario of a client transition

Empower SCVAT, Inc., world's largest hotel chain to focus on hospitality, innovations and service delivery that is secure and compliant by design using SSDL to transform security from a bottleneck to an enabler.

Client Objective 

SCVAT, Inc. is the world's largest hotel chain with a need for enhanced cloud security architecture and DevSecOps embed into every phase of development across its multi-cloud platforms



Our Solution 

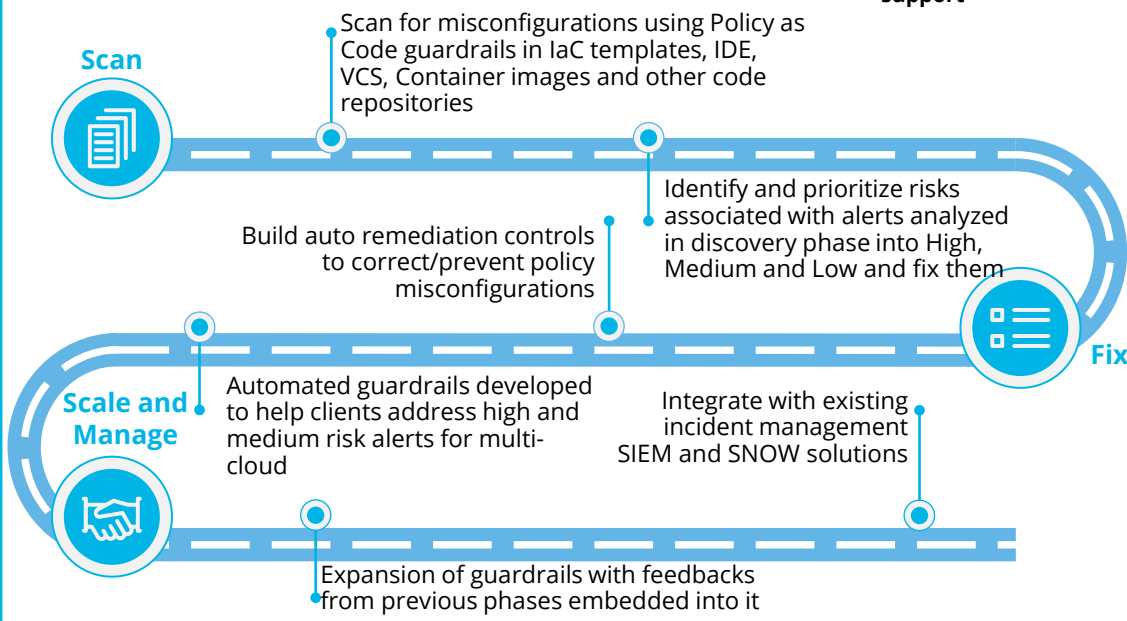
Implement SSDL to embed security checks across each phase of DevOps lifecycle to enable detection and remediation of misconfigurations in the early stages of development


Understand the current security posture of their multi-cloud environment through cloud security scans and understand the governance, compliance and business specific requirements to be implemented in the security roadmap


Develop detailed architecture pattern, define guardrails for implementation of security controls and prioritize high-risk alerts to develop tailored guardrails on the identified security data points


Deploy Policy as Code guardrails deployed with industry leading best practices, Deloitte secure guardrails, compliance requirements, cloud governance and strategy requirements and organization's custom requirements in design, build and monitor phases


Our Approach   **5 Professionals for implementation**
6-9 Professionals for support





Scan  Scan for misconfigurations using Policy as Code guardrails in IaC templates, IDE, VCS, Container images and other code repositories

Build auto remediation controls  Build auto remediation controls to correct/prevent policy misconfigurations






Identify and prioritize risks  Identify and prioritize risks associated with alerts analyzed in discovery phase into High, Medium and Low and fix them

Scale and Manage  Automated guardrails developed to help clients address high and medium risk alerts for multi-cloud

Integrate with existing incident management  Integrate with existing incident management SIEM and SNOW solutions

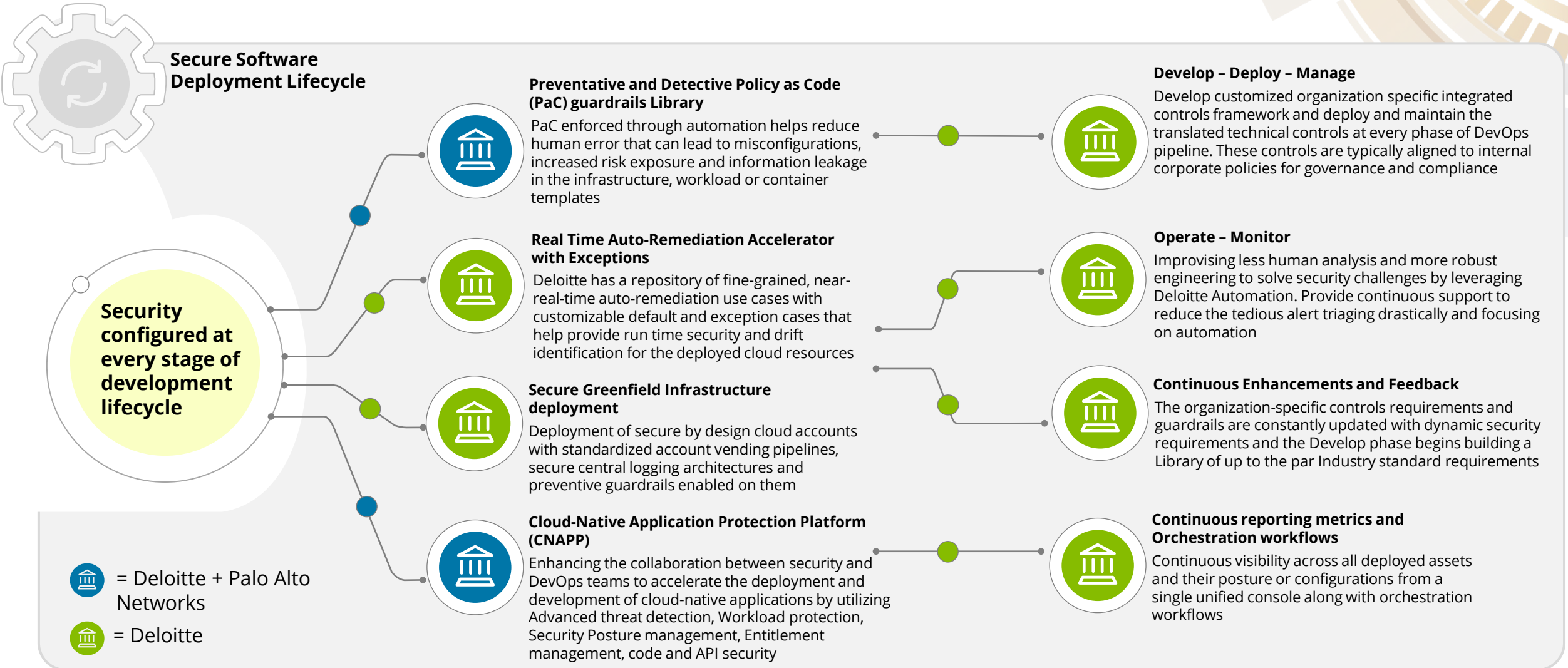
Fix  Expansion of guardrails with feedbacks from previous phases embedded into it

Innovation and Continuous Improvement

-  Efficient integration with multi-cloud platforms
-  Prohibit the deployment of misconfigured resources into the environment
-  Continuously monitors for configuration deviations
-  Decreases costs related to compliance (HIPPA, CIS, etc.,) activities
-  Establish visibility to cloud infrastructure security

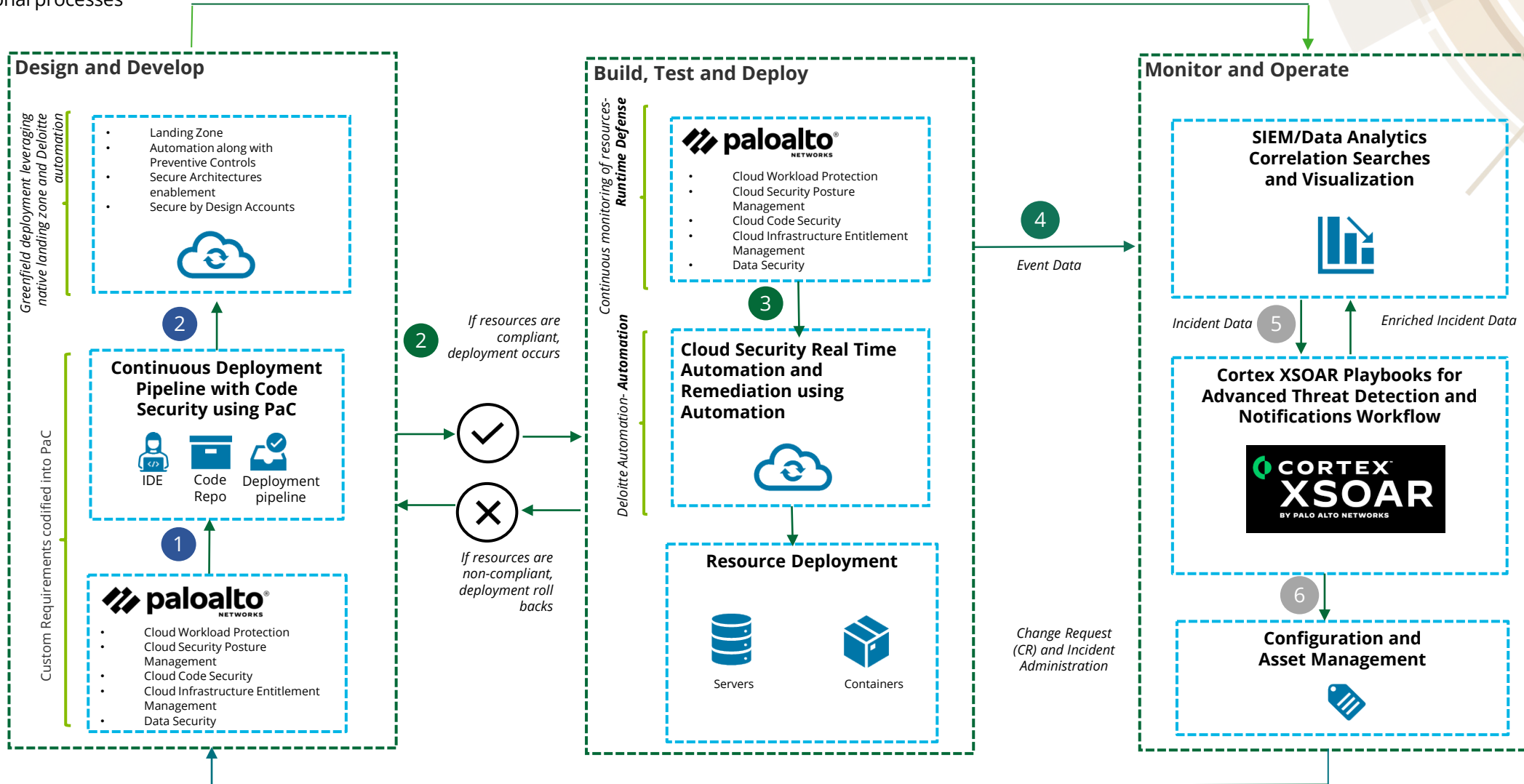
SSDL accelerators

SSDL is designed to help you to enforce and manage governance rules for security, operations, and compliance at scale across all your organizations, resources, workloads and pipelines



End-to-end SSDL

Below are the components and capabilities to enable our SSDL across the cloud landscape to mitigate cloud service vulnerabilities and improve security operational processes



The approach for deploying SSDL



Approach for enabling SSDL

2 weeks

Strategy planning

- Identify stakeholders
- Obtain access to existing documentations, architecture patterns, blueprints
- If CSPM solution exists, obtain access and current state configurations (If no CSPM solution exists, assist client with performing proof of concept (POC), procurement, design and implementation *)
- Conduct knowledge transfer sessions from client team to understand the multi-cloud environment to confirm the setup of cloud native services (e.g., Landing Zone, Centralized Logging architecture and Service Control Policies or Guardrails)
- Conduct workshops to discuss the client DevOps tool chain (e.g., CI/CD pipeline, Integrated Development Environment, Version Control System, Imager Builder, Container Image repository) and the integrations
- Obtain list of multi-cloud services currently used, third-party tools integration (SIEM, SOAR and ITSM) within the multi-cloud environment
- Understand the security and compliance requirements, review latest version of client's control framework and align to the prioritized security risk domains for control policy development

2 weeks

Initial development and preparation activities

- Perform sprint planning activities with the client point-of-contact
- Conduct backlog refinement
- Onboard the CSPM tool or refine the existing one by enabling and onboarding the in-scope multi-cloud accounts.
- Perform Post-Installation setup of CSPM tool as per client requirements
- Align with the organization specific cloud control framework and identify prioritized policies and security risk domains
- Obtain access to client's cloud environments, existing CI/CD pipeline, tool chains and to existing documentations and configuration guides
- Define coding standards and baseline configurations for the in-scope services
- Identify list of prioritized use cases from Iron Dome's repository of ~1629 use cases (129 custom + 1500 out of the box) and default policies for CSPM, Cloud Code Security, CIEM and CWP modules per client's security and compliance requirements
- Develop architecture pattern covering the five (5) security risk domains

4 weeks

Build, deploy and test

- **Enablement of CSPM, Cloud Code Security, CWP and CIEM modules**
- Enable existing CSPM, Code Security, CIEM, CWPPs out of the box policies as per organization security policy
- Setup runtime environment scans for all workloads by installing defender agents or agentless scanning as per client's ecosystem and configuration management processes
- Develop or onboard up to 40 new custom Policy as Code guardrails in CSPM, Cloud Code Security, CIEM and CWP module as per organizational requirements
- Develop process flows for the security risk domains
- Conduct User Acceptance Testing
- **Greenfield setup**
- Fine tune existing greenfield environment (if any) with enablement of Service Control Policies or Guardrails, centralized account vending architecture and logging architecture (or we will setup a secure greenfield environment from scratch*)
- Enable cloud native security services and subscribe it to master audit account
- Fix the alerts from CSPM tool by developing customized remediation automations in development environment for the in-scope security risk domains based on automation user stories
- Perform testing in the development environment along with User Acceptance Testing

4 weeks

Integrate and transition

- Perform integration with cloud operations and DevOps tools (e.g., SIEM, SOAR and ITSM, CI/CD pipeline) for the developed automation scripts and with CSPM and other modules
- Build advanced security orchestration workflows with SOAR with customizations to triage an incident and notify necessary stakeholders of crucial events
- Develop knowledge base (KB) articles
- Develop documentations such as runbooks and configuration guides
- Develop advanced dashboards to provide single pane of glass view across all platform alerts such as CSPM, CWP, CIEM, Cloud Code Security and Automation accelerators to enable data driven insights that will provide metrics such as path to green and intel on top violators

Activities

Outcomes

- | | | | |
|---|---|---|--|
| <ul style="list-style-type: none"> • Stakeholder list • Finalized CSPM tool and compliance requirements • Prioritized list of in-scope services, accounts, tool chains and documentations • Cloud control framework aligned to in-scope security risk domains | <ul style="list-style-type: none"> • Sprint plan • Prioritized list of use cases • Architecture patterns • Onboarded accounts and fine tuning of CSPM per custom requirements | <ul style="list-style-type: none"> • Finalized policies and use cases enabled across CSPM, CIEM, CWP, Cloud Code Security and custom automation code scripts for the in-scope services • Process workflows • User Acceptance Testing | <ul style="list-style-type: none"> • Integration with cloud operations and DevOps tools • Orchestration Playbooks • Configuration guides and runbooks • KB articles • Automation and orchestration reporting dashboards |
|---|---|---|--|

Contact



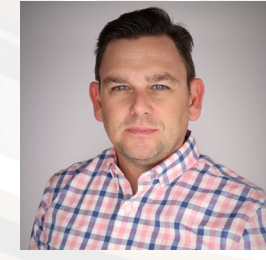
Kieran Norton
Advisory Principal
Deloitte and Touche LLP
+1 (415) 783 5382
kinorton@deloitte.com



Jane Chung
Advisory Managing Director
Deloitte and Touche LLP
+1 (408) 704 4524
jachung@deloitte.com



Varsha Vithal Kakati
Advisory Sr. Vice President
Deloitte and Touche Assurance
and Enterprise Risk Services
India Private Limited
+1 (470) 434 2373
vkakati@deloitte.com



Cary Hickerson
Deloitte Services LP
Advisory Senior Manager
+1 (303) 305 3050
chickerson@deloitte.com



Siddharth Kantroo
Deloitte and Touche LLP
Advisory Senior Manager
+1 (615) 718 1347
skantroo@deloitte.com



Lenox Edwards
Deloitte Services LLP
Advisory Manager
+1 (212) 436 7552
leedwards@deloitte.com



Mahithaa Sree Moganti
Advisory Solution Advisor
Deloitte and Touche Assurance
and Enterprise Risk Services India
Private Limited
+1 (615) 718 9204
mmahithaasree@deloitte.com



Akshaya Jeyachandran
Solution Delivery Associate
Deloitte and Touche
Assurance and Enterprise
Risk Services India Private
Limited
+1 (615) 718 3112
jakshaya@deloitte.com

Appendix



SSDL offering objectives

Below are the capabilities to help establish continuous compliance for a multi-cloud environment.

Design and Develop

1. **Policy as Code-** Guardrails configured at every stage of development cycle codified with industry leading practices, Deloitte secure guardrails, compliance requirements, cloud governance and strategy requirements and organization's custom requirements
2. **Secrets Scanning-** Scanning of secrets in code and container repositories
3. **Secure Greenfield deployment-** Leveraging native cloud landing zone accelerators and Deloitte automation
4. **Secure Deployment Templates-** Preconfigured secure deployment templates for cloud workloads

Build, Test and Deploy

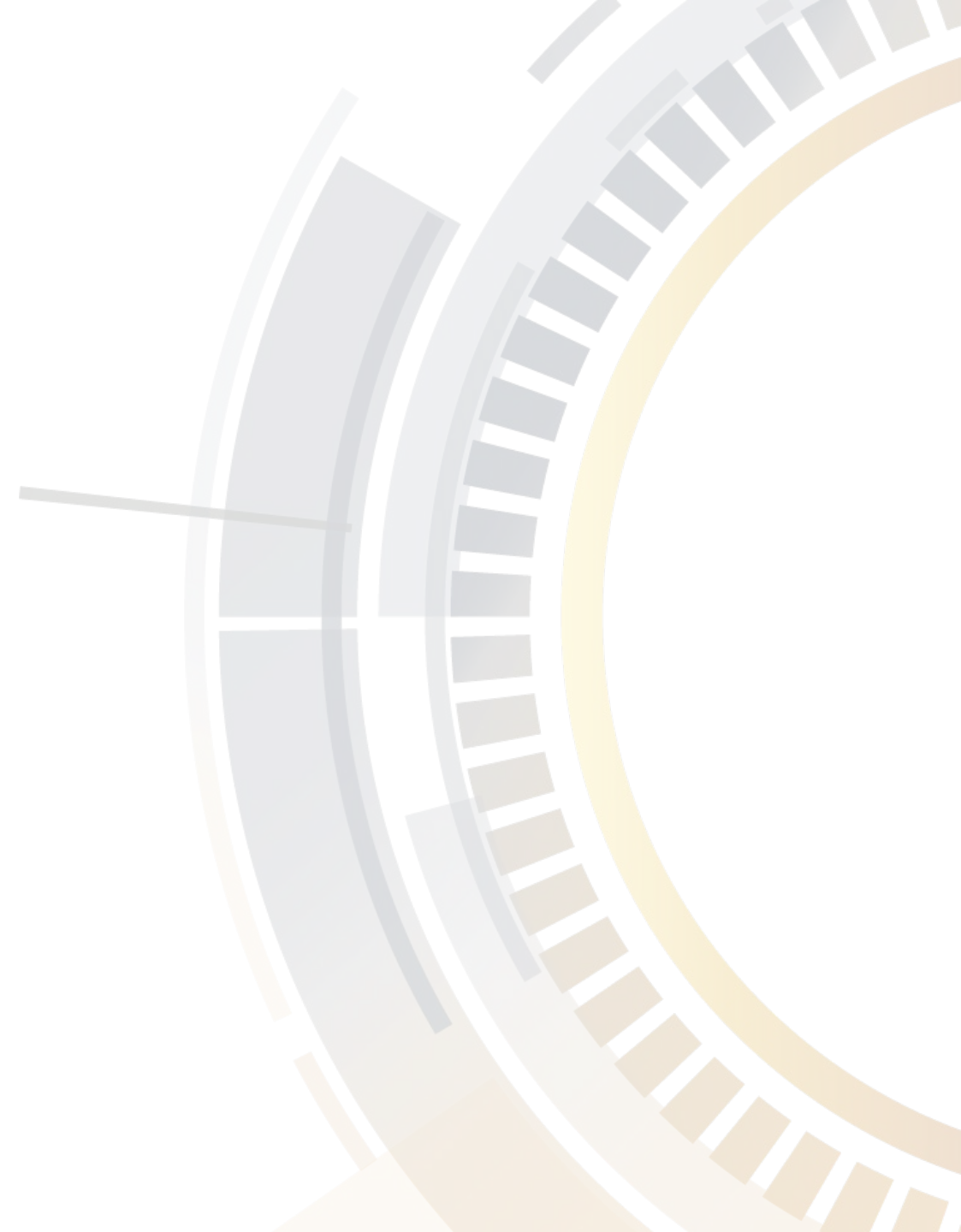
1. **Misconfigured deployment rollback and feedbacks-** Failure of insecure deployments on cloud with rollback to the previous stage along with recommendations for fixes
2. **Continuous monitoring of deployed resources along with auto remediation-** Runtime Defense for workloads, containers, infrastructure and entitlements and baseline remediations
3. **Advanced Behavior Analysis-** Establish User entity behavior analytics (UEBA) - monitor cloud environments for unusual user activities
4. **Segregation of duties-** Access controls for segregation of duties and authorization tollgates to review and accept build requests

Monitor and Operate

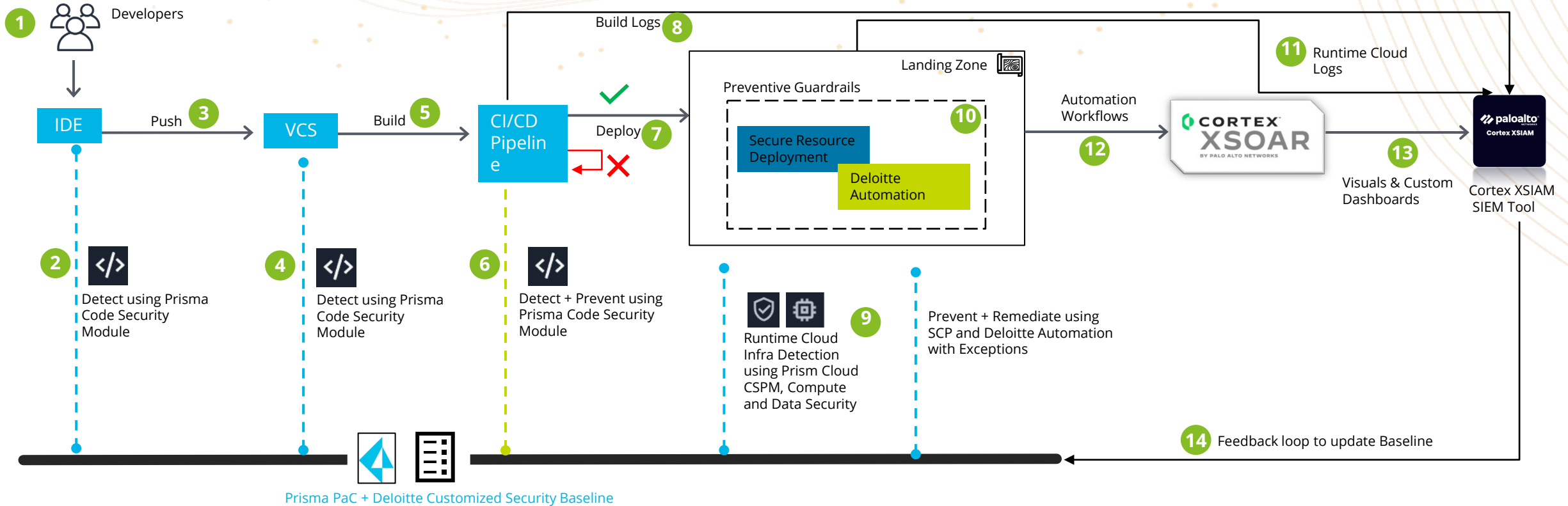
1. **Continuous reporting metrics-** Establish continuous visibility across all deployed assets and their posture or configurations from a single unified console
2. **Advanced Correlation searches-** Real time analysis of alerts and discovery of unusual activities and insider threats or potential account compromises
3. **Orchestration workflows-** Implement orchestration playbooks and automation workflows
4. **Expansion of security landscape-** Continuous feedback to the security baselines



Demonstration



SSDL conceptual architecture



- Developers designing and developing the code in IDE
- Early detection of misconfigurations for Infrastructure as Code in IDE scanned against Policy as Code baseline security baseline by using Prisma checkov scanner
- Developed code is pushed into Version Control System (VCS)
- Real time detection of code misconfigurations in VCS and real time with conditional fixes in place by using Prisma checkov scanner. Can suppress low severity findings and fix the prioritized findings
- Code from VCS is pushed into CI/CD pipeline for build & deploy
- Detective with Preventative controls enforced on the CI/CD pipeline limiting the unsecure deployment into cloud environment and to adhere continuous compliance by using Prisma checkov scanner
- Secure deployment is performed upon passing the security baseline checks else the deployment fails to enforce consistent, complaint and secure deployments
- Failed pipeline CI/CD logs are sent to SIEM tool for DevOps team to better collaborate and improve agility
- In the runtime cloud environment, any drift, vulnerability, misconfigurations can be identified real-time using Prisma Cloud CSPM, Compute & Data Security with remediation using Deloitte Automation in place along with Detection and prevention
- Runtime cloud environment now has secure deployments with preventive custom cloud guardrails in place to avoid runtime modification with real time automation and exceptions in place. Includes Secure Account Vending component.
- Runtime misconfigurations are sent to SIEM tool for DevOps team to better collaborate and improve agility
- Orchestration workflows with Cortex XSOAR for case management, notifications and advanced automation workflows
- Near Real time monitoring in SIEM tool for a unified view of all the reporting metrics
- Any new security mis configuration identified in the SIEM tool will be shared in a feedback loops for PaC Security baseline enhancements

SSDL functional use case overview

ID	Domain	Functional Use Case	Description
1	Infrastructure Security	Control access of an authorized Kubernetes-user	Detect and alert/block if a user performs other than the actions which are not validated by a custom Kubernetes role in a namespace.
2	Infrastructure Security	Control resource accessibility by a pod in a cluster	Detect and alert/block if the newly created pods are using the default service account not the custom one mapped with custom IAM Role.
3	Infrastructure Security	Control deployment of resources with labels	Control the scope of the policy rules by checking the object's metadata, such as namespace with labels.
4	Infrastructure Security	Controlled exposition of applications using Ingress	Alert or detect if a pod or the deployment is assuming the same role (assigned through default service account) as one assigned to the node/nodegroup
5	Infrastructure Security	Generate alert whenever new user is added to config file	Alert or detect if a new user is added to Config File
6	Infrastructure Security	Image Scanning with packer for container	Scanning of container images though the use of Packer
7	Infrastructure Security	Restrict container image coming from untrusted repo	Detect and alert/block if container image is coming from untrusted repositories (the ones which are not specified by the organization).
8	Infrastructure Security	Control pod cpu/memory request and limit	Detect and alert if pod cpu/memory utilization crosses the set-threshold
9	Infrastructure Security	Control admission/validation of pods through custom pod security policy	Detect and alert if a pod is admitted and validated against default 'pod security policy' which by default allows complete access.
10	Infrastructure Security	Tag Quarantining	To check if workloads present in the cloud environment have organization approved tags attached to them
11	Network Security	Auto Host Replacement	To automate replacement of hosts which get infected by users through malicious commands.
12	Infrastructure Security	Image scanning with Packer for Host	Scanning of host images using Packer
13	Network Security	Forbidden Datatype Blocking	Filtering out unexpected datatypes in request can help us from vulnerability and potential system instability
14	Network Security	Payload Limiting	Preventing large payloads from reaching our server can help us mitigate the risk of downtime and unauthenticated access.
15	Network Security	Sensitive Data Protection	Exploiting a vulnerability might lead the API to leak sensitive data to the attacker but with a custom rule scanning the outgoing data the sensitive data will be stopped from going forward to the attacker.

SSDL functional use case overview

ID	Domain	Functional Use Case	Description
16	Identity and Access Management	Privileged Escalation Detective Control	Preventing attackers from impersonating other roles or gain permissions they should not have.
17	Identity and Access Management	Role assumed via CLI	To identify if any Highly privileged IAM roles are being assumed through CLI by IAM Local Users or Identity Center Users in cloud Account.
18	Identity and Access Management	RAM Resource share	To identify if resources are being shared to external principals.
19	Identity and Access Management	Breakglass User Validation	To track and identify a break-glass user's activity to ensure he is not performing routine tasks such as ConsoleLogin
20	Identity and Access Management	Permission Boundaries (Roles) and Users	To identify users for whom Permission Boundary does not exist and to ensure permissions attached with permission boundaries do not allow high privileges
21	Identity and Access Management	SCIM Event	To identify if SCIM events are performed by Local IAM Users or SSO Users
22	Identity and Access Management	CloudFormation stacks with High Privileged Role	To identify if any Cloudformation stacks have been created with highly privileged service roles.
23	Data Security	Checks if a REST API stage uses a Secure Sockets Layer (SSL) certificate.	To ensure that REST API stage uses an SSL certificate in order to maintain data encryption
24	Data Security	Checks if Amazon S3 buckets have policies that require requests to use Secure Socket Layer (SSL)- runtime covered by Prisma	S3 bucket policy should not allow HTTP requests for data and network security. HTTPS is a secure way of communication on the internet.
25	Infrastructure Security	Ensure that AMIs are not shared publicly	Check for publicly shared AMIs using resource block ami_launch_permissions. The group value should not be equal to all.
26	Data Security	Bulk Operations (BULK DELETE)	To alert the system when a bulk delete occurs and remediate the incident by Restricting access to the entity that performed bulk delete.
27	Data Security	Sensitive Data Detection EC2	To alert the system if any sensitive data is stored in EC2 instances



Thank you.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Product names mentioned in this presentation are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Inclusion does not constitute an endorsement of the product and/or service. Deloitte & Touche LLP is not responsible for the functionality or technology related to the Vendor or other systems or technologies as defined in this presentation.



As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

**Copyright ©2023 Deloitte Development LLC.
All rights reserved. Member of Deloitte Touche Tohmatsu Limited**