HITACHI
Inspire the Next

CNCJ: Cloud Native Security Japan LT祭り

クラウドネイティブ時代のセキュリティ戦略 — CNAPPの機能解剖

Dec. 04, 2024

Takaya Ide

Services Computing Research Dept.
Center for Digital Service - Digital Platform Center
Research & Development Group, Hitachi, Ltd.

クラウドネイティブのセキュリティ

クラウドネイティブのセキュリティ対策は難化の一途

- システムの複雑化、分散化
- 巨大なエコシステム上の様々な要素が関与
- 開発高速化やデプロイ頻度の増加
- アプリケーションやミドルウェアの頻繁な更新
- 境界防御からゼロトラストセキュリティへの推移
- セキュリティ攻撃の多様化

- 一方で、セキュリティがアジリティを阻害することは望ましくない

CNCF, “CLOUD NATIVE SECURITY WHITEPAPER”, 2022

HITACHI
Inspire the Next

CNAPP: Gartnerが提唱するクラウドネイティブ向けの包括的なセキュリティ基盤構想

- 開発・運用ライフサイクル全体に渡るセキュリティを一元的に提供するプラットフォーム
  - ◇ 知見不足に対策漏れの抑止
  - ◇ 複雑さの低減、適用・管理の省力化
- 構成要素
  - ◇ Artifact Scanning
    ソースコードやバイナリなどの検証
  - ◇ Cloud Configuration
    インフラ環境の構成チェック
  - ◇ Runtime Protection
    稼働中のシステムに対する攻撃検知・防御

CNAPP: Cloud Native Application Protection Platform

Artifact Scanning

- SAST/DAST
- API Scanning
- Software Composition Analysis
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Attack Path Analysis

Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Settlements Management
- Kubernetes Security Posture Management
- Cloud Security Posture Management

Runtime Protection

- Web Application and API Protection
- Application Monitoring
- Cloud Workload Protection Platform
- Network Segmentation
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Attack Path Analysis

“Innovation Insight for Cloud-Native Application Protection Platforms”, Gartner, 2021 の図を参考に作図

CNAPPを扱う上での懸念

HITACHI
Inspire the Next

CNAPPに含まれる機能の規定がなく、人ごとにスコープが異なる

- オリジナルの文書はCNAPPの構想の解説がメインであり、構成する機能は規定しない
- CNAPPの構成要素自体が複合的な概念であるため、機能が部分的に重複
  - ASPM, SCA, 脆弱性スキャン, 脆弱性管理
  - Data Security, Data Protection, DSPM
  - CSPMにIaC Scanningは含むのか

→ CNAPPの構成機能が曖昧で、意思疎通やツールの比較などが困難

CNAPP機能リスト

HITACHI
Inspire the Next

市場調査をもとにCNAPPの機能要素をリスト化

作成手順

1. GartnerによるガイドラインおよびCNAPPに取り組んでいるセキュリティベンダ7社の資料を調査し、
   複数ベンダがCNAPPとして共通的に扱っている機能をリストアップ
   → この時点では粒度や名称違いの機能が複数混入

2. 各機能を対象フェーズ(実装、テスト、デプロイ等)、リソース(アプリ、データ、OS等)、機能カテゴリで分類し、
   重複や粒度違いの機能を整理

→ 46種のセキュリティ機能※に抽出。以降でリストを紹介

※ 日立として内容を保証するものではない。リスト自体は随時更新する運用

※ アラートなど全てのセキュリティで共通的な機能は除いて記載

Artifact scanning

HITACHI
Inspire the Next

カテゴリ	#	機能	説明	フェーズ
ASPM (Application Security Posture Management)	1	SAST (Static Application Security Testing)	ソースコードの静的解析による脆弱性診断	Test
	2	DAST (Dynamic App. Security Testing)	試験的にアプリを攻撃する脆弱性診断	Test
	3	IAST (Interactive App. Security Testing)	アプリ内エージェントにて通信から脆弱性診断を行う	Test
-	4	API Scanning	APIの仕様や脆弱性を診断	Test
SCA※ (Software Composition Analysis)	5	Vulnerability Scanning	ライブラリに含まれる既知の脆弱性を検出	Test
	6	License Scanning	ライブラリのライセンスを検出	Test
Exposure Scanning	7	Compliance Check	コンプライアンスに反して公開されているコンポーネントの検出	Test
	8	Secrets Scanning	アクセスキー等の機密情報の扱いの診断	Test
	9	Sensitive Data Scanning	個人情報等の扱いの診断	Test
	10	Malware Scanning	マルウェアの検出	Test
	11	Attack Path Analysis	通信トポロジー等に基づく攻撃経路の予測	Deploy

※ SCAもASPMの一部

Cloud configuration

カテゴリ	#	機能	説明	フェーズ
-	12	IaC Scanning	Ansible等の設定ミスや脆弱性の検出	Test
CSPM (Cloud Security Posture management)	13	Benchmarking	知識ベースでの欠陥や脆弱性の検出	Deploy/Operate
	14	Compliance Check	コンプライアンス違反の検出	Deploy/Operate
	15	Drift Detection	設定変更の検出	Deploy/Operate
	16	Provide Guided Remediation	修正方法の提案	Deploy/Operate
	17	Visualization	状態の可視化	Deploy/Operate
CIEM (Cloud Infrastructure Entitlements Management)	18	Permission Management	権限付与状況の可視化	Deploy/Operate
	19	Improper Authorization Detecting	不必要に割り当てられた権限の検出	Deploy/Operate
	20	Suspicious Account Blocking	不正アカウントのブロック	Deploy/Operate

Runtime protection (1/2)

HITACHI
Inspire the Next

カテゴリ	#	機能	説明	フェーズ
WAAP (Web Application /API Protection)	21	WAF (Web Application Firewall)	XSSやSQL Injectionなどの攻撃の遮断	Operate
	22	Threat Detection	入出力や振舞い監視による脅威検出	Operate
	23	Bot Prevention	Botによるスクレイピング等の防御	Operate
	24	DDoS Protection	DDoSの検知とブロック	Operate
	25	Authorization	HTTPヘッダ等に基づくAPIの認可制御	Operate
Micro Segmentation	26	Network Authorization	コンテナ間通信の認可制御	Operate
CSNS (Cloud Service Network Security)	27	Threat Protection	脅威の侵入や横方向への展開の抑止	Operate
	28	Exposure Management	外部公開されているデータの検出および制御	Operate
	29	Thread Detection	トラフィックに基づく脅威検知	Operate
	30	Traffic Topology Map	通信関係の可視化	Operate
	31	Traffic Encryption	通信の暗号化	Operate
CWPP (Cloud Workload Protection Platform)	32	Runtime Protection	振る舞いベースの脅威検出	Operate
	33	Malware Detection	システム内のマルウェア検知・隔離	Operate
	34	Intrusion Prevention	侵入防止	Operate

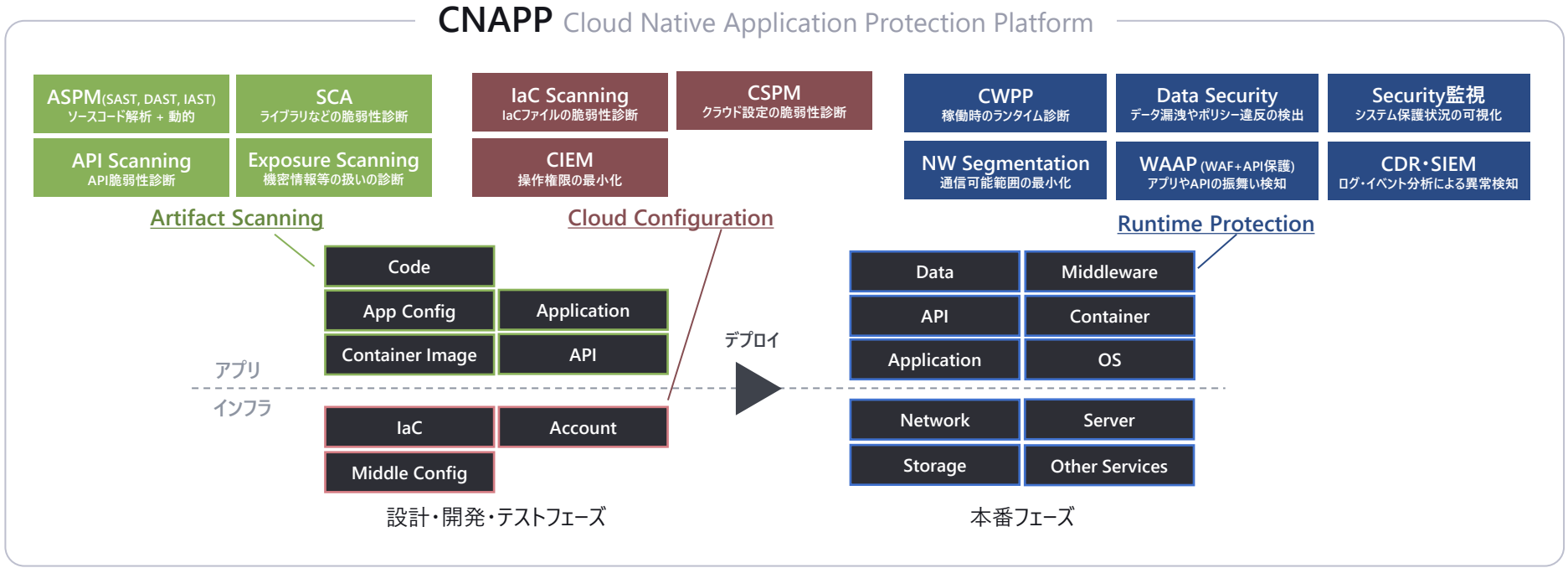
Runtime protection (2/2)

HITACHI
Inspire the Next

カテゴリ	#	機能	説明	フェーズ
CWPP (Cloud Workload Protection Platform)	35	Unauthorized Access Detection	不正アクセスの検知	Operate
	36	Vulnerability Scanning	脆弱性診断	Operate
	37	Compliance Check	コンプライアンス違反の検出	Operate
	38	Visualize	セキュリティ事故の経緯や原因の分析	Operate
SOAR (Security Orchestration, Automation and Response)	39	Security Incident Management	インシデント情報の収集と管理	Operate
	40	Security Automation	インシデント対処の自動化	Operate
SIEM (Security Information and Event Management)	41	Thread Detection	複数ログの相関付けや振る舞い分析による脅威検出	Operate
	42	Compliance Check	ログベースでのコンプライアンス違反の検出	
Data Security (DSPM; Data Security Posture Management とも)	43	DLP (Data Loss Prevention)	機密データの漏洩や盗難の防止	Operate
	44	Compliance Check	データ管理状況(GDPR違反など)などのチェック	Operate
	45	Unauthorized File Detection	不正ファイルの検出	Operate
	46	Visualization	データや規制状況の可視化	Operate

まとめ

- Gartnerは開発・運用に跨った包括的なセキュリテ基盤構想 CNAPP を提唱
- CNAPPを構成する機能のリストを作成



Trademarks

- Gartner is a trademark of G. G. Properties, Ltd. in the United States and/or other countries.