

ランタイムセキュリティ徹底解剖！ デモで体感振る舞い検知

2023年6月15日
Sysdig Japan合同会社
Mac Kawabata



スピーカー紹介



川端 真
Mac Kawabata
兵庫県尼崎市出身
犬好き、餃子の王将好き

職歴	職種
大王製紙	プラントエンジニア
ネットワンシステムズ	ネットワークエンジニア
EMC	ストレージエンジニア
Crossbeam Systems	セキュリティエンジニア
Nutanix	日本法人立ち上げ
Nimble Storage	日本法人立ち上げ
HPE	ストレージプリセールス長
AWS	ストレージスペシャリスト
Sysdig	チャンネル&アライアンス責任者

Sysdigとは？

WireSharkの作者、Loris Degioanniにより2013年に創業
可視化、トラブルシューティング、セキュリティの向上を
より幅広い人々に届けるために、オープンな姿勢を貫くカルチャーの会社



Monitoring

Security

Founded by the creator of

WIRESHARK

プロトコル解析と
ネットワークセキュリティ

Sysdig | Open Source

ディープコンテナ
フォレンジックと
トラブルシューティング

Falco

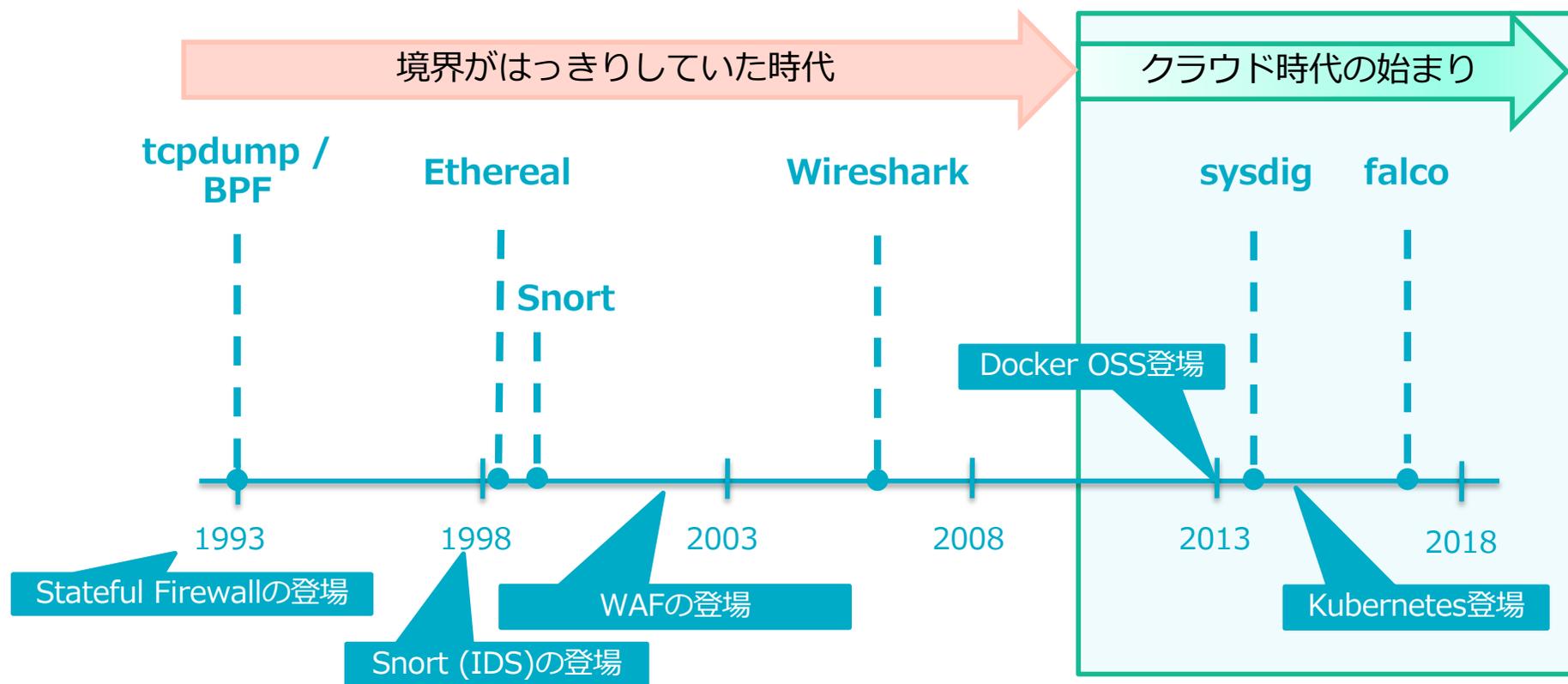
クラウドネイティブの
脅威と異常の検知



☆ ~5k GitHub stars ↓ 60M downloads

Yahoo!Japan、メルカリ、NTT-Data等、
多くの国内ユーザー事例有り！

ちょっと歴史の振り返り



今までの境界型セキュリティ



ファイアウォールで守られた
明確な入口が存在した



侵入検知をする事でセキュリティ
が担保されていた



オンプレミス時代のスタンダード

境界の存在しない最先端環境のセキュリティ



クラウド事業者が
外部との接続を保有



クラウドは世界中からのアクセス
に晒されている



サービスへのアクセスコントロー
ルはユーザー側の責任



怪しい振る舞いを検知するのも
ユーザー側の責任



攻撃手段の多様化により、もはや境界の定義は困難に。。。

境界のない世界では、強固な扉や鍵よりも セキュリティカメラが重要



 不審な変更の監視

 侵入者や内部からの不審な
振る舞いの検知

 迅速なアラートの検知と迅
速なアクションによる被害
の最小化



振る舞い検知のデファクトスタンダードFalco

The screenshot shows the 'Our incubating projects' section of the CNCF website. The page features a grid of 20 project cards, each with a logo, name, and brief description. The Falco project is highlighted with a red border. The grid is organized as follows:

Project Name	Category
Backstage	Application Definition & Image Build
Buildpacks.io	Application Definition & Image Build
OPA (Open Policy Agent)	Security & Compliance
Chaos Mesh	Chaos Engineering
cilium	Cloud Native Network
Cloud Custodian	Automation & Configuration
cloudevents	Streaming & Messaging
CNI	Cloud Native Network
CONTOUR	Service Proxy
cortex	Monitoring
cri-o	Container Runtime
Crossplane	Scheduling & Orchestration
CubeFS	Cloud Native Storage
dapr	Framework
Dragonfly	Container Registry
EMISSARY INGRESS	API Gateway
Falco	Security & Compliance
gRPC	Remote Procedure Call
in-toto	Security & Compliance
Istio	Service Mesh





Falco: クラウドネイティブ脅威検知のデファクトスタンダード

6,000万^{以上}

ダウンロード数

100社^{以上}

貢献企業

Falco エンドユーザー



BOSE



VOLVO

SAMSUNG



StateFarm

Uber

Walmart *

幅広い業界での採用



Fargate ランタイムセキュリティ

Google

gVisor サーバレスセキュリティ



シスフローのテレメトリーとセキュリティ



Defenderデータの収集



Data収集

sumo logic 異常検出

O'REILLY®

Practical Cloud Native Security with Falco

Risk and Threat Detection for Containers, Kubernetes, and Cloud



Sponsored by
 **sysdig**

Loris Degioanni
& Leonardo Grasso



CNAPPとは？

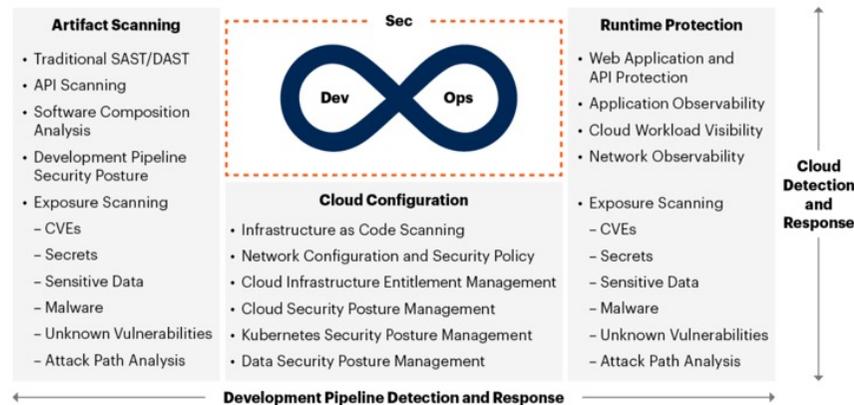
Cloud Native Application Protection Platforms (CNAPPs) combine functionality for Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), Cloud Infrastructure Entitlement Management (CIEM), and Cloud Detection and Response (CDR) security into one security platform. These integrated capabilities allow DevOps to ship applications fast without security becoming a bottleneck while also allowing security teams to manage risk and defend against attacks.

クラウドネイティブアプリケーション保護プラットフォーム (CNAPP) は、

- クラウドセキュリティポスチャ管理 (CSPM) 、
- クラウドワークロード保護 (CWP) 、
- クラウド基盤権限管理 (CIEM) 、
- クラウド検知/レスポンス (CDR)

これらのセキュリティの機能を1つのセキュリティプラットフォームとして統合し、それによりDevOpsはセキュリティをネックとせずにアプリケーションを迅速に出荷できる一方、セキュリティチームはリスクを管理し攻撃を防御できるようになります。

CNAPP Detailed View



CVEs = common vulnerabilities and exposures
 Source: Gartner
 785751_C

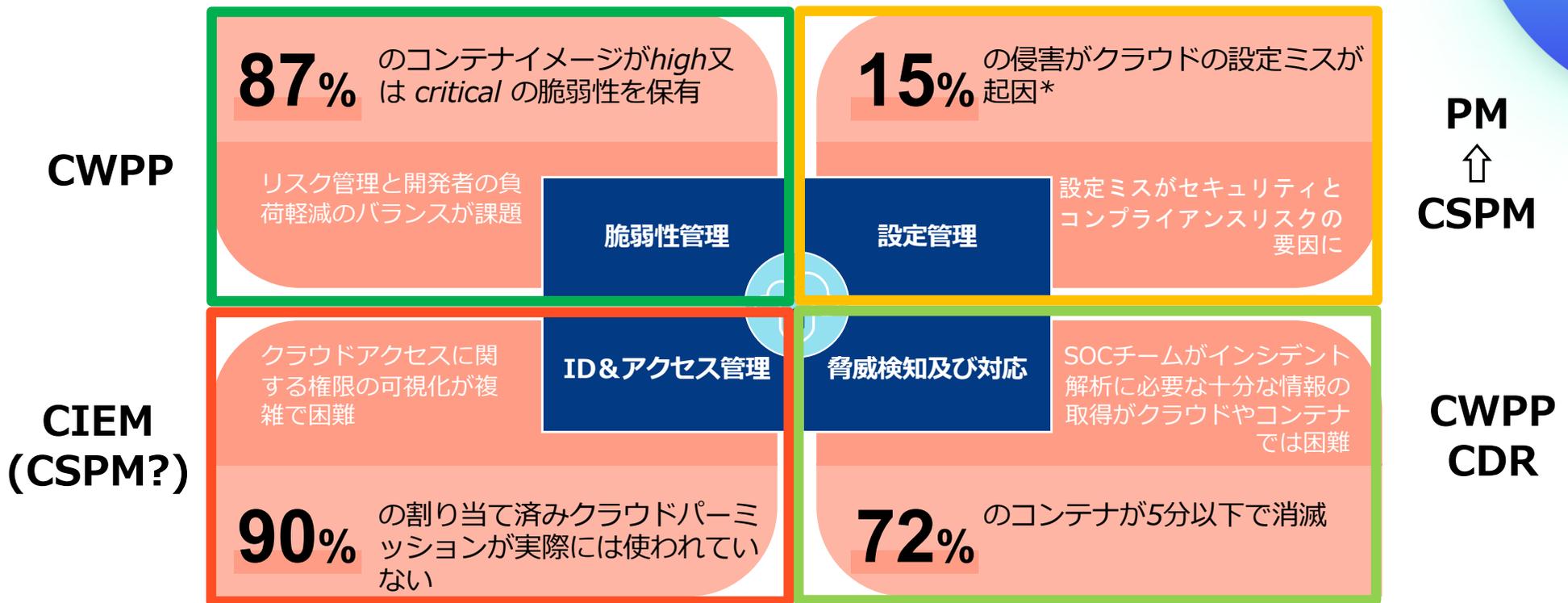
Gartner

$$\text{CNAPP} \doteq \text{CWPP} + \text{CSPM}$$



* 出展 : [Gartner Market Guide for 2023 – 6 key takeaways](#)

クラウドネイティブセキュリティ4つのポイント



何をしようが攻撃は受けます



軍隊



国家



組織化されたプロ

では完全にお手上げなのか？



現実世界同様、攻撃には偵察が必要



MITRE ATT&CK って知ってますか？

MITRE ATT&CK™ Navigator

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Binary Padding	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	BITS Jobs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shim	Clear Command History	Credentials in Files	Exploitation for Credential Access	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Authentication Package	Code Signing	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	BITS Jobs	Compiled HTML File	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Module Load	Bootkit	Component Firmware	Component Object Model Hijacking	Hooking	Network Sniffing	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Control Panel Items	Input Capture	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Change Default File Association	Dylib Hijacking	DCShadow	Input Prompt	Peripheral Device Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Component Firmware	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Keychain	Process Discovery	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content			Port Knocking
	Mshst	Dylib Hijacking	Launch Daemon	Exploitation for Defense Evasion	Password Filter DLL	Security Software Discovery	Third-party Software			Remote Access Tools
	PowerShell	External Remote Services	New Service	Extra Window Memory Injection	Private Keys	System Information Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	File System Permissions Weakness	Path Interception	File Deletion	Securityd Memory	System Network Configuration Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	Hidden Files and Directories	Plist Modification	File Permissions Modification	Two-Factor Authentication Interception	System Network Connections Discovery				Standard Cryptographic Protocol
	Rundll32	Hooking	Port Monitors	File System Logical Offsets		System Owner/User Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hypervisor	Process Injection	Gatekeeper Bypass						Uncommonly Used Port
	Scripting	Image File Execution Options Injection	Scheduled Task	Hidden Files and Directories						Web Service
	Service Execution	Kernel Modules and Drivers	Service Registry Permissions Weakness	Hidden Users						
	Signed Binary Proxy Execution			Hidden Window						
	Signed Script Proxy Execution									

jack.mitre.org

Sateird

^ legend



Falco MITRE Rule Matrix

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration
DB program spawned process	Modify Shell Configuration File	Launch Privileged Container	Clear Log Activities	Read sensitive file trusted after startup	Read Shell Configuration File	Launch Privileged Container	System proc network activity
Run shell untrusted	Schedule Cron Jobs	Non sudo setuid	Delete Bash History	Read sensitive file untrusted	Read ssh information	Launch Suspicious Mount Container	Interpreted proc inbound network activity
Terminal shell in container	Update Package Repository			Search Private Keys or Passwords	Read sensitive file untrusted	Launch Disallowed Container	Interpreted proc outbound network activity
Neical Remote Code Execution in Container	Write below binary dir Write below monitored dir				Contact K8S API Server From Container		Unexpected UDP Traffic
	Write below etc Write below root Write below rpm database				Launch Suspicious Network Tool in Container		Launch Suspicious Network Tool in Container
	Modify binary dirs Mkdir binary dirs				Launch Suspicious Network Tool on Host		Launch Suspicious Network Tool on Host
	User mount binaries						
	Create files below dev						
	Launch Package Management Process in Container						
	Remove Bulk Data from Disk Set						
	Create Hidden Files or Directories						
	Setuid or Setoid bit						

sysdig mitre で検索！



デジタル世界のセキュリティカメラ

オープン
テクノロジー + エージェント
ベース + リアルタイム
脅威検知



DEMO



Cloud and Container Security
from Source to Run