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

sysdig

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

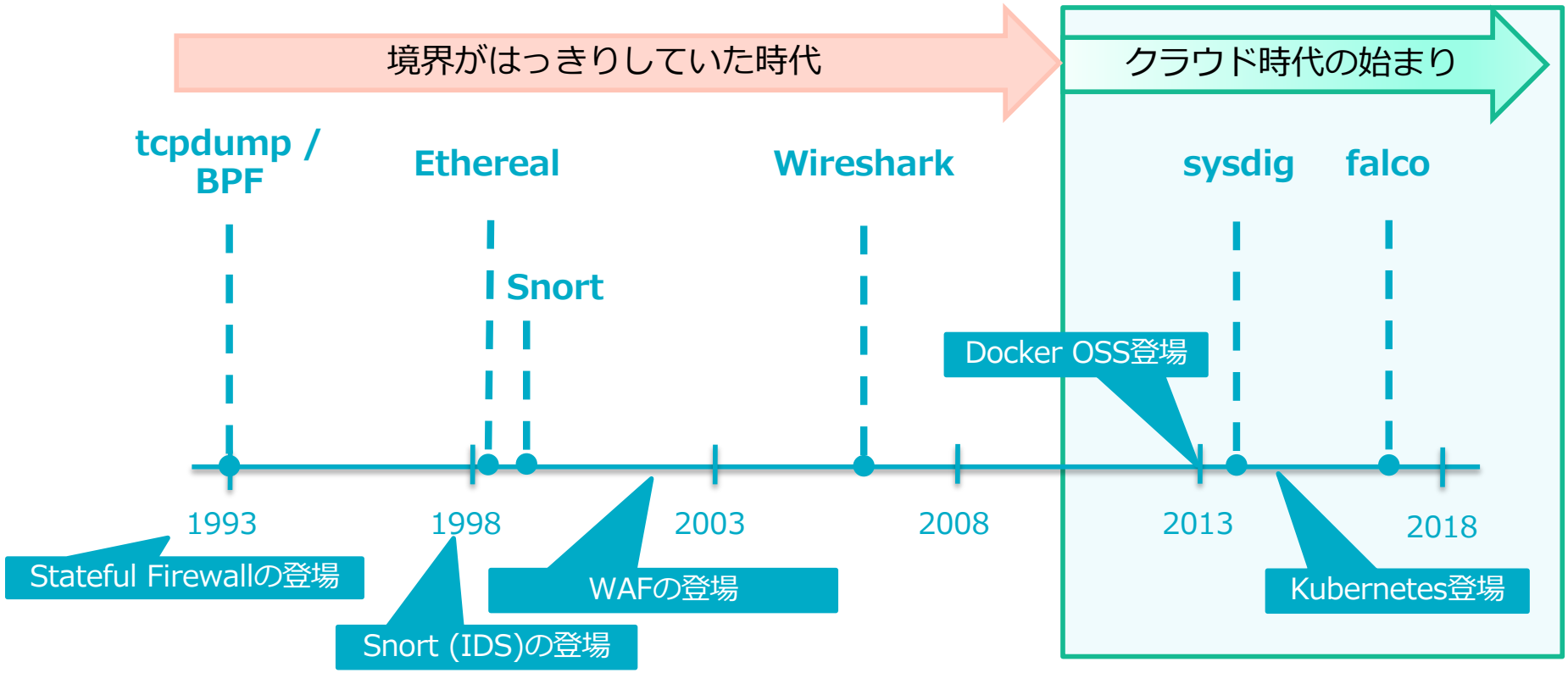
Sysdig Open Source
ディープコンテナ
フォレンジックと
トラブルシューティング

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

sysdig

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

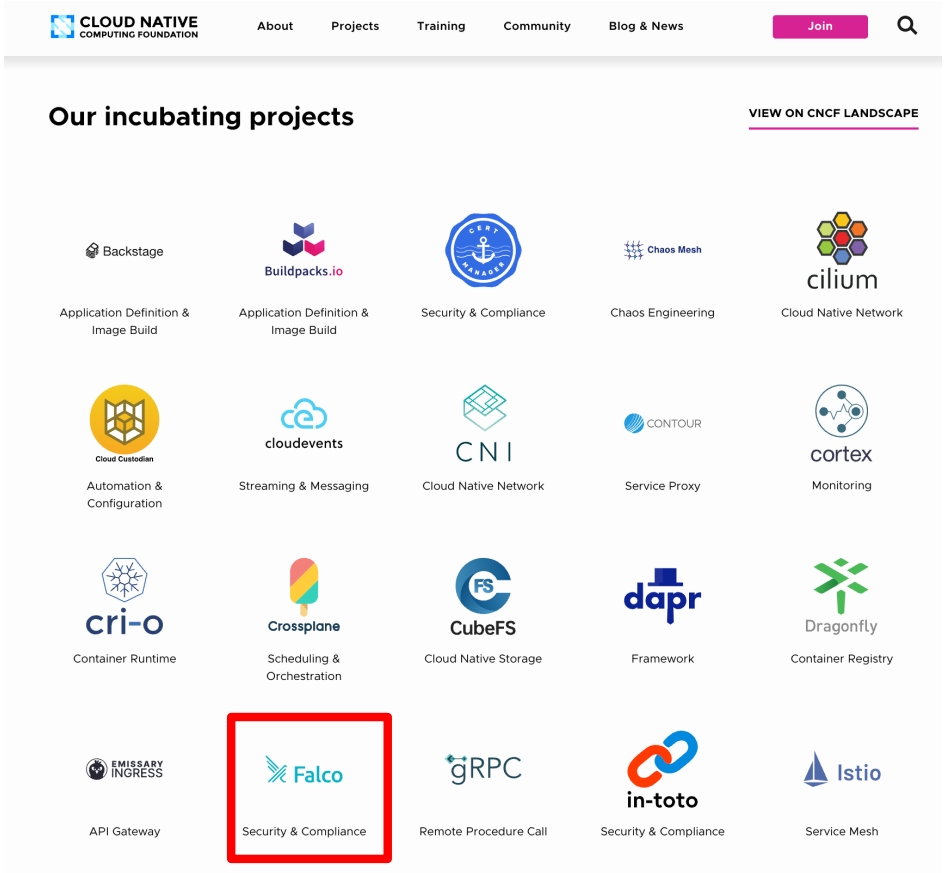
攻撃手段の多様化により、もはや境界の定義は困難に。。。

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

sysdig

振る舞い検知のデファクトスタンダードFalco



sysdig

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

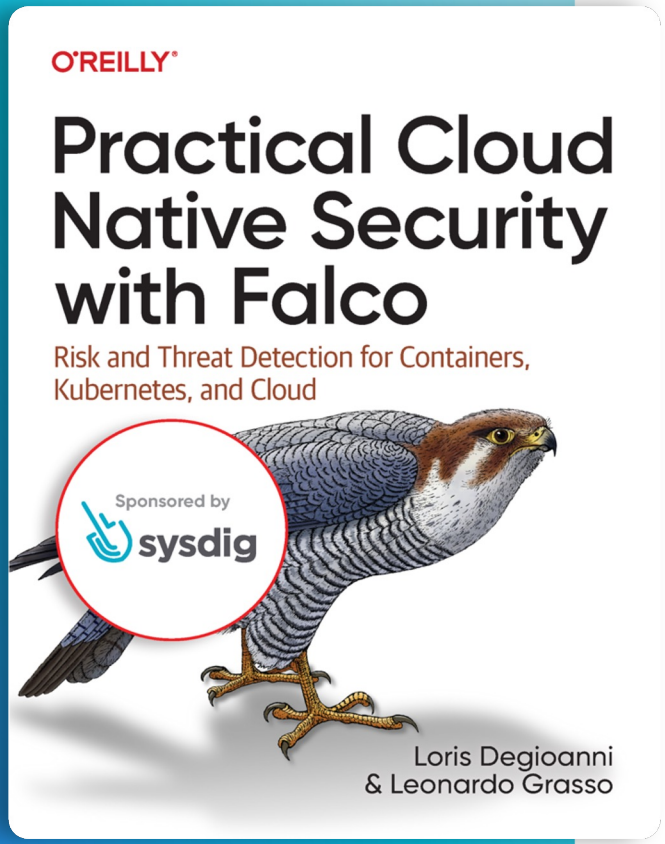
6,000万以上
ダウンロード数

100社以上
貢献企業

Falco エンドユーザー

幅広い業界での採用

aws	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
IBM	シスフローのテレメトリーとセキュリティ
Microsoft	Defenderデータの収集
Red Hat	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


pwc
sysdig
Make Progress
Thrive in

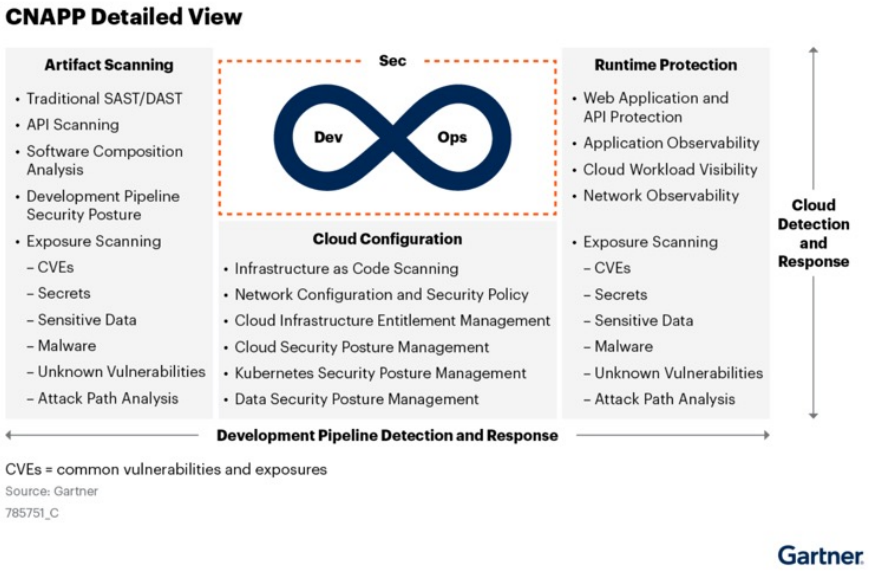
sysdig

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）

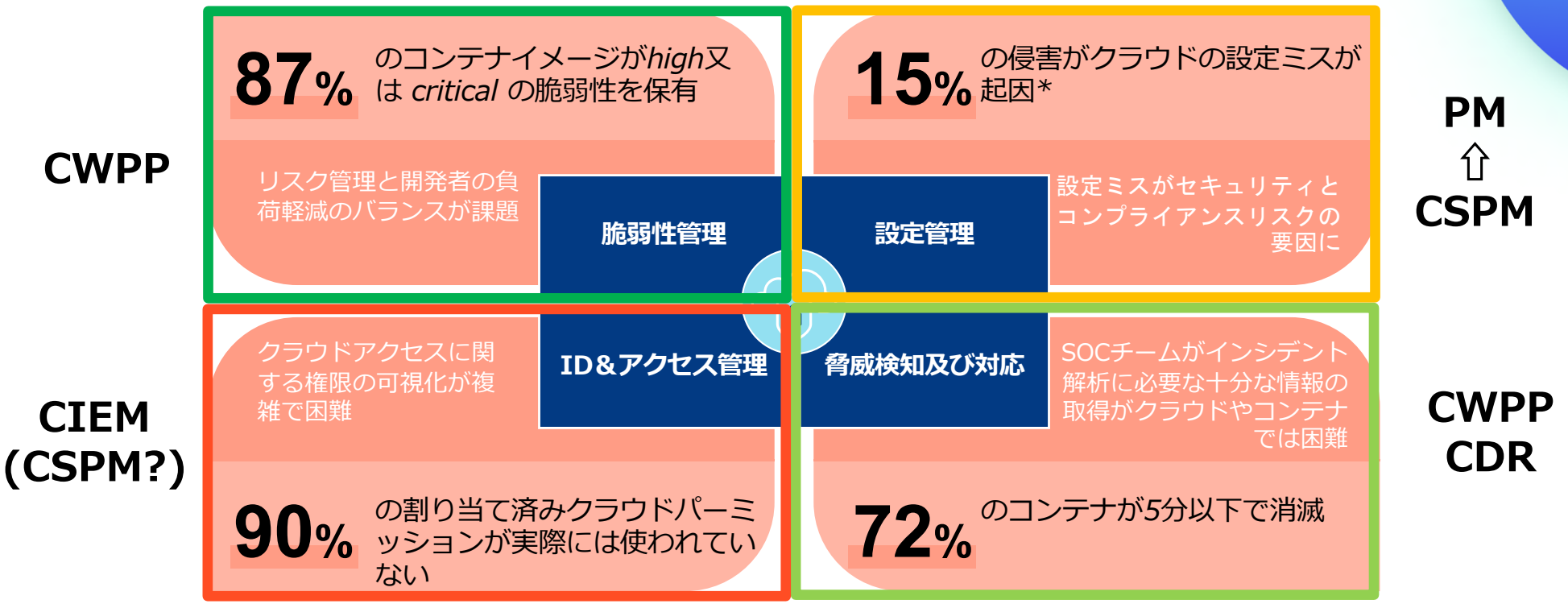
これらのセキュリティの機能を1つのセキュリティプラットフォームとして統合し、それによりDevOpsはセキュリティをネックとせずに
アプリケーションを迅速に出荷できる一方、セキュリティチームは
リスクを管理し攻撃を防御できるようになります。



CNAPP ≒ CWPP + 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



sysdig

Sysdig 2023 Container Security and Usage Report
*IBM 2022 Cost of a Breach report

何をしようが攻撃は受けます

軍隊

国家

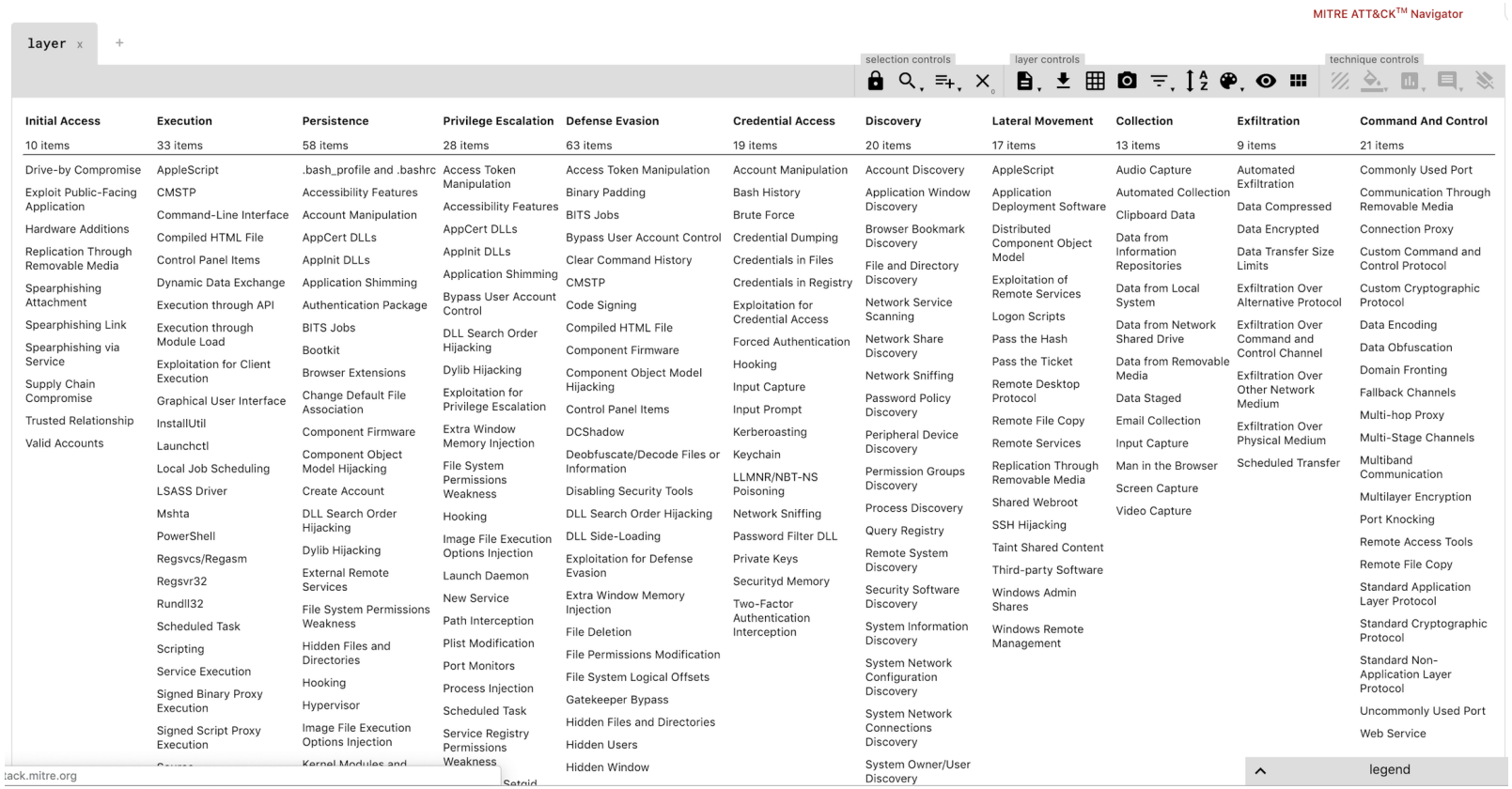
組織化されたプロ

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

sysdig

MITRE ATT&CK って知ってますか？



sysdig

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 procs network activity
Run shell untrusted	Schedule Cron Jobs	Non sudo setuid	Delete Bash History	Read sensitive file untrusted	Read ssh information	Launch Sensitive Mount Container	Interpreted procs inbound network activity
Terminal shell in container	Update Package Repository			Search Private Keys or Passwords	Read sensitive file untrusted	Launch Disallowed Container	Interpreted procs outbound network activity
Netcat 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 mgmt binaries						
	Create files below dev						
	Launch Package Management Process in Container						
	Remove Bulk Data from Disk Set						
	Create Hidden Files or Directories						
	Setuid or Setgid bit						

sysdig mitre で検索！

sysdig

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