SOC FORUM 2023

LUNTRY

SOC в контейнерах

Дмитрий Евдокимов
Founder, CTO Luntry

Обо мне

SOC FORUM 2023

- Основатель и технический директор Luntry
- Опыт в ИБ более 10 лет
- Специализация безопасность контейнеров и Kubernetes
- Программный комитет конференция DevOpsConf , HighLoad++
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Автор Telegram-канала “k8s (in)security”
- Автор курса “Cloud Native безопасность в Kubernetes”
- Не верит, что систему можно сделать надежной и безопасной, не понимая ее
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, KuberConf, VK Kubernetes Conference, HighLoad++, DevOops , БЕКОН и др.

Дмитрий Евдокимов
Founder&CTO Luntry

План доклада

SOC FORUM 2023

- Окружение
- DFIR
- Специфика DFIR в k8s
  - Проблемы
  - Преимущества

Результат моего общения с командами SOC

SOC FORUM 2023

Все SOC не любят/ненавидят окружения с контейнерами, Kubernetes и прочей новомодной нечестью =)

Простейший тест

SOC FORUM 2023

Вопросы:

1. Что такое StaticPod?
2. Почему полезно следить за Pods без metadata.ownerReferences?
3. О чем говорит обращение к ресурсу SelfSubjectAccessReview от ServiceAccount микросервиса?

Окружение

Окружение

SOC
FORUM
2023

Окружение

SOC
FORUM
2023

Окружение

SOC
FORUM
2023

Окружение

kubernetes

Окружение

kubernetes

Окружение

SOC FORUM 2023

kubernetes

Platform as a Service (PaaS)

- Configuration
- Functions
- Applications
- Runtime
- Containers
- Operating Systems
- Hardware

Yandex Cloud

VK Cloud Solutions

SBER CLOUD

Окружение

kubernetes

Platform as a Service (PaaS)

- Configuration
- Functions
- Applications
- Runtime
- Containers
- Operating Systems
- Hardware

Yandex Cloud

VK Cloud Solutions

SBER CLOUD

Разработчики

DevOps

SRE

Аналитики

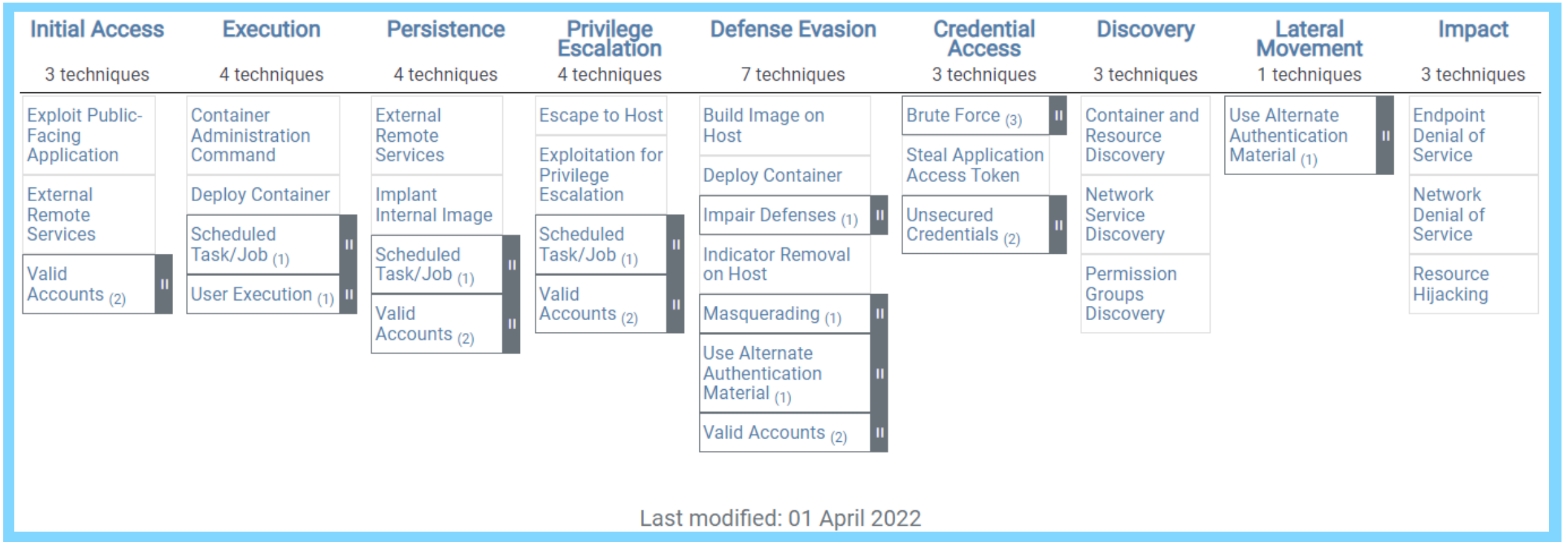
QA

Monitoring

DFIR в k8s

MITRE ATT&CK Containers Matrix

SOC FORUM 2023



Link

Threat matrix для Kubernetes от Microsoft

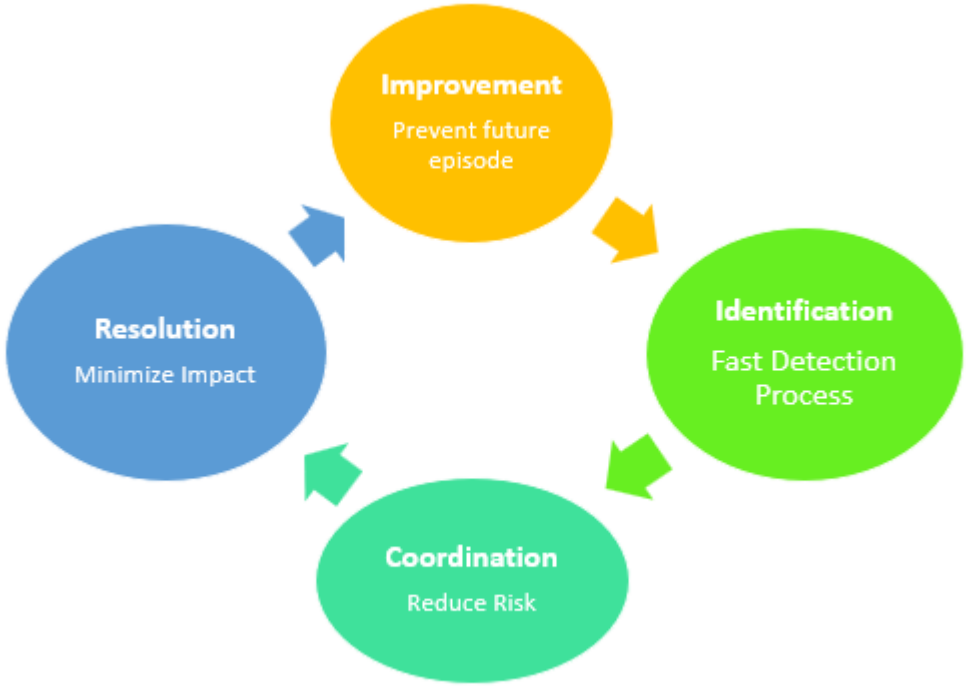
SOC FORUM 2023

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access Kubernetes API server	Access cloud resources	Images from a private registry	Data destruction
Compromised image In registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Collecting data from pod	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from proxy server	Application credentials in configuration files	Exposed sensitive interfaces	Application credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container	Container service account			Access managed identity credentials	Instance Metadata API	Writable hostPath mount		
	Sidecar injection	Static pods			Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

DFIR (Digital Forensics and Incident Response)

SOC FORUM 2023

- DFIR Live
  - Container
- DFIR Offline
  - Logs
  - Dumps



Incident Response Plan

IR в Kubernetes

SOC FORUM 2023

Incident Response

While incident response is primarily a human process, in this section we discuss how Kuberenetes policy management impacts it. Kubernetes incident response should be aligned with established DevSecOps operating principles with an emphasis on recognizing the declarative state, ephemeral nature of workloads, and automated controls.

Kubernetes and cloud native technologies introduce new challenges for planning incident response. The volume of telemetry data required to effectively identify and detect attacks is larger due to the short lifespan of containers, and since the persistence of resources is not guaranteed. Telemetry and audit logs need to be ingested and processed automatically instead of manual review and enrichment so that automation workflows can manage and respond to operational status changes in the infrastructure by extracting actionable events out of raw telemetry data. Existing SIEM and SOAR platforms may not be up to the challenge, having focused on manual human operations.

Increasing adoption of Chaos Engineering into Kubernetes incident response planning and simulation helps surface new threats and design better monitors and telemetry ingestion flows. ML-based telemetry analysis can help proactively identify anomaly scenarios and edge cases. It is increasingly important to build automated remediation, using policy-as-code, and to curate and train ML models so that these tools adapt as attackers evolve. Kubernetes policy reports can provide additional data, with long term data collected and stored in the PAP.

“Kubernetes Policy Management”

Проблемы SOC в k8s

Проблема №0: Обнаружить инцидент в контейнере

SOC FORUM 2023

- Подходы базирующиеся на правилах и сигнатурах работают очень плохо
  - Происходящее в контейнерах меняется от компании к компании
    - Уникальная логика каждого микросервиса
    - Сложно к чему-то привязаться
  - “Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks” Intezer, 2020
  - “Bypassing Falco: How to Compromise a Cluster without Tripping the SOC“ Shay Berkovich (BlackBerry), 2022

Проблема №1: Традиционные инструменты не понимают контейнеры

SOC FORUM 2023

- Устоявший стек решений не подходит
  - Необходимо различать контейнерные процессы от хостовых
  - Необходимо группировать активность по контейнерам
  - Необходимо понимать, что за образ используется в контейнере в конкретный момент времени
  - Необходимо сопоставлять контейнеры с высокоуровневыми абстракциями/сущностями Kubernetes (Pod, Deployment, DaemonSet, …)
  - Необходимо в Kubernetes ориентироваться в Resources и Subresources
- Нужно использовать Cloud-native решения

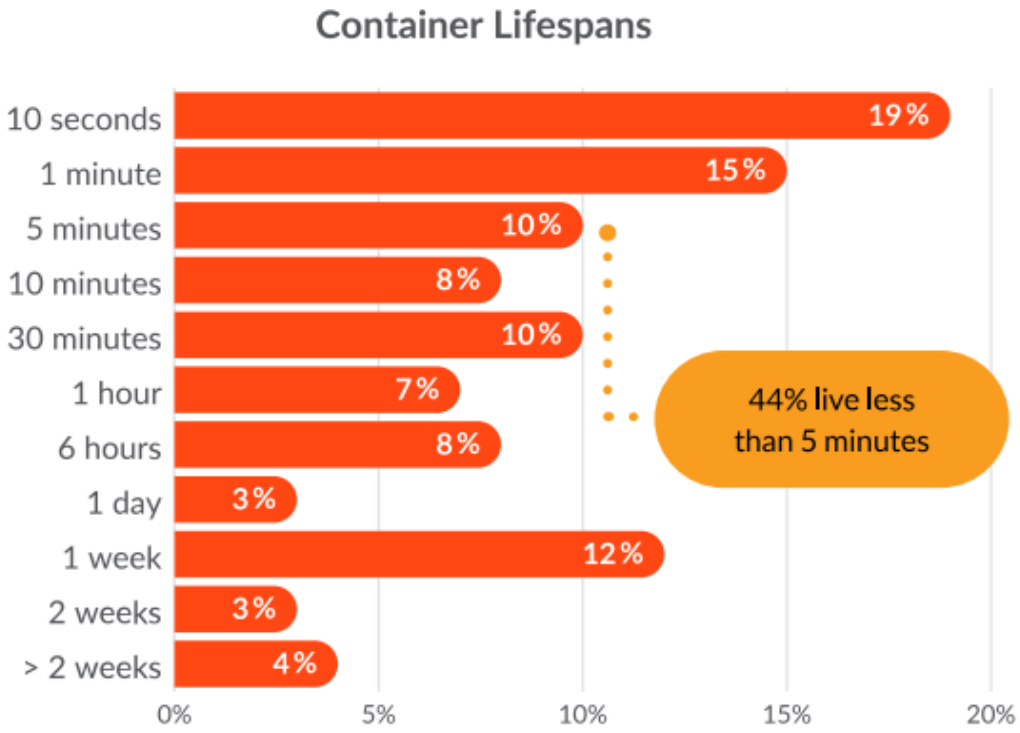
Проблема №2: Высокие требования к оверхедам

SOC FORUM 2023

- Привет HighLoad!
  - Сильное отличие от пользовательских рабочих станций
- Как в процессе сбора, обработки информации, так и при ее хранении
  - CPU
    - Никто не хочет замедлять свои микросервисы
    - Никто не хочет отдавать много процессорных ядер под агенты на Nodes
  - Memory
    - Агенты генерируют большой объем данных

Проблема №3: Динамическое окружение

SOC FORUM 2023

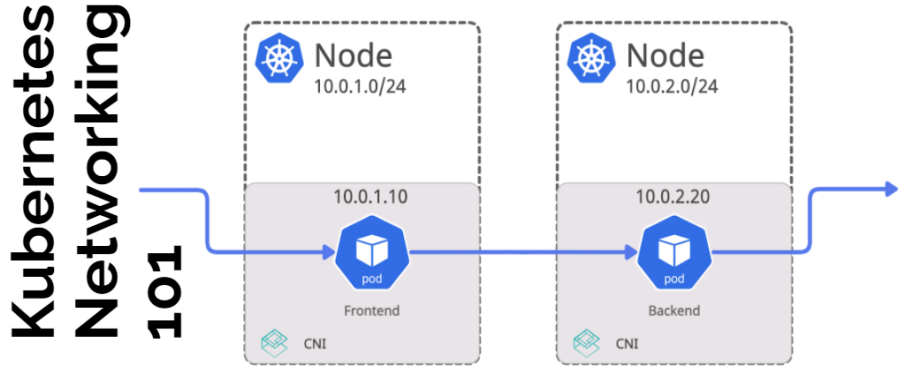


[“Sysdig 2022 Cloud-Native Security and Usage Report”]

- Малый срок жизни контейнеров
  - Большое количество обновлений
  - Self-healing
  - Переезд контейнеров с Node на Node
  - Появление новых Nodes и копий контейнеров при автоскейлинге
  - …
- Следы злоумышленника в контейнере почистятся сами собой!

Проблема №4: Специфика сетевого взаимодействия в k8s

SOC FORUM 2023



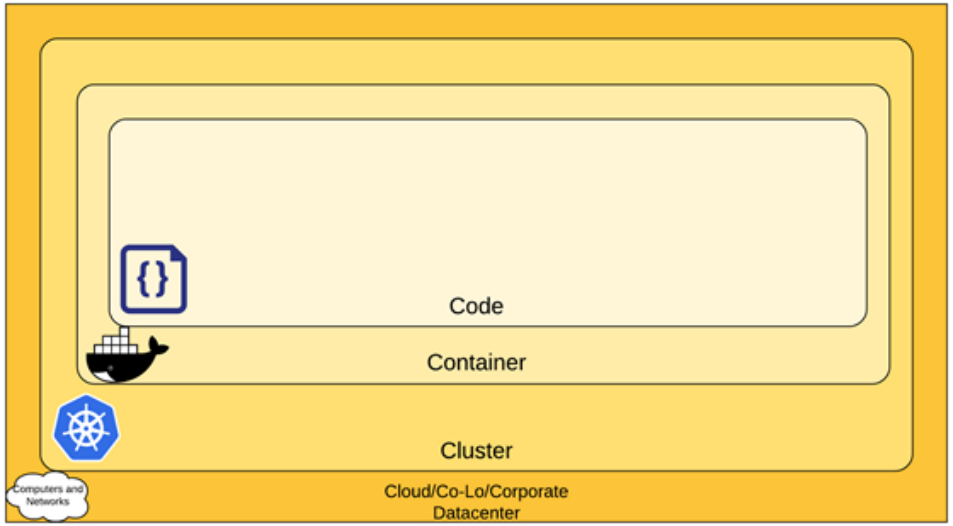
- All Pods have IPs
- All Pods can talk
- PodCIDR[s] per node

- Services for load-balancing
- DNS for service-discovery
- Network Policy for segmentation

- IP адрес меняется/переходит от запуска к запуску контейнеров
  - Нельзя строить корреляцию на основе только IP адресов

Проблема №5: Множество уровней абстракций

SOC FORUM 2023



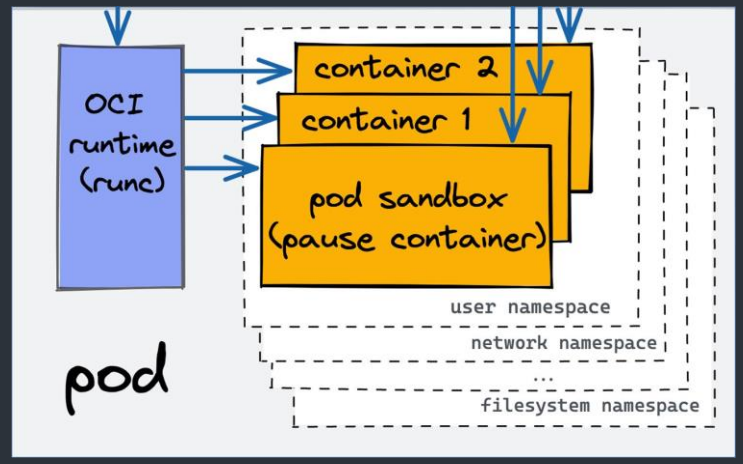
- Kubernetes это PaaS и каждый нижележащий уровень абстрагирован от другого
  - Четкое разделение на Control plane и workloads
- OS
  - OS Log
- Application
  - App log
- Containers
  - Runtime
  - Memory и FS dump
- Kubernetes cluster
  - Kubernetes Audit Log
- Cloud/Datacenter
  - Log

Преимущества k8s для SOC

Преимущество #1: Контейнеры это не rocket science ;)

SOC FORUM 2023

- Классический Container = Linux process + cgroup + namespaces (pid, user, uts, ipc, net, mnt, …) + pivot_root + image
  - Изоляция
  - Образ
- Можно работать как с обычными процессами и частью файловой системы хоста

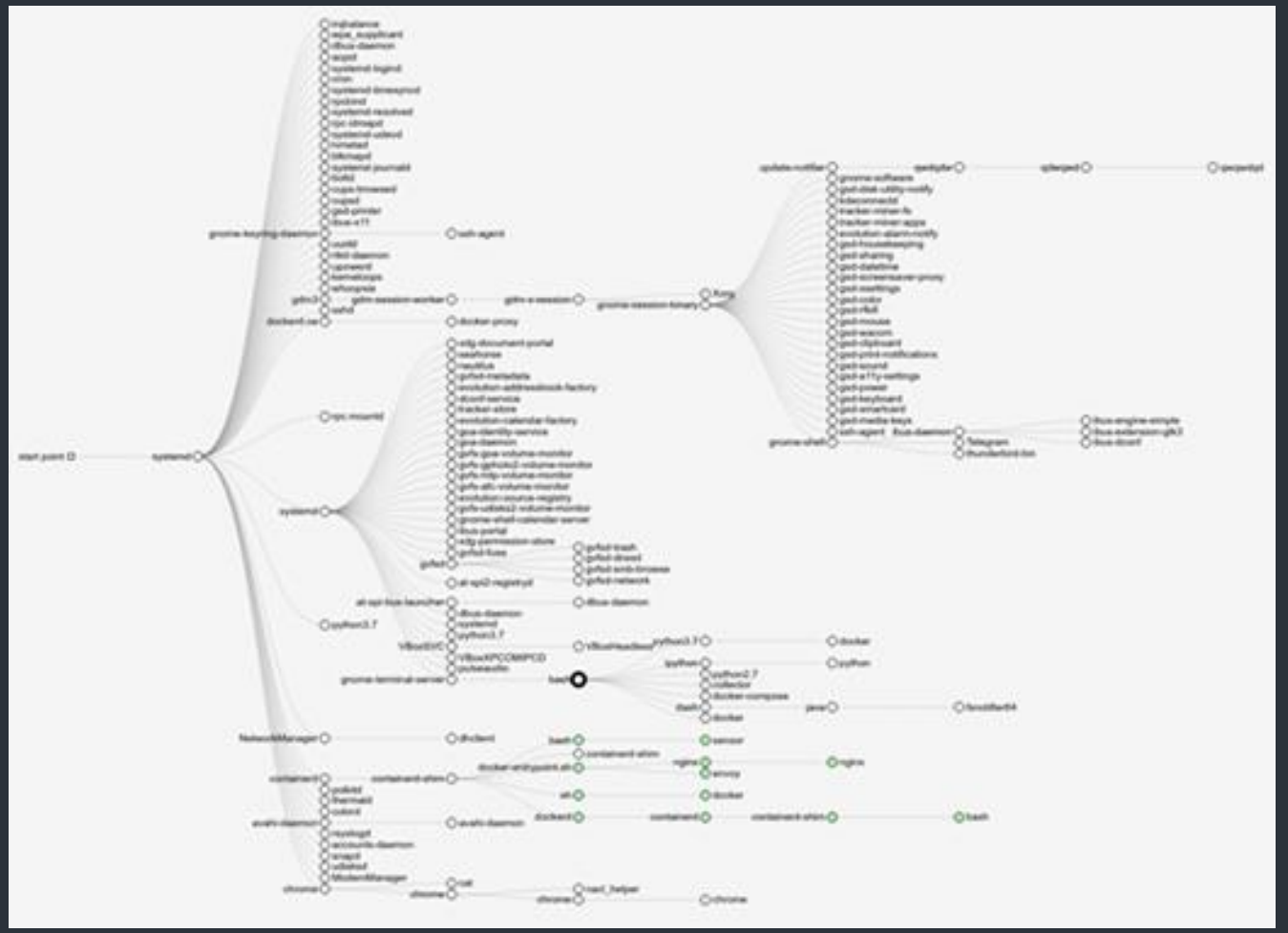



```
root      598309  0.0  0.0 110128  6224 ?        Sl   Nov20   0:07  \_ containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1
root      598334  1.4  5.5 7236340 1832196 pts/0 Ssl+ Nov20  39:39      \_ /docker-java-home/bin/java -Djava.util.logging.config.file=/opt/atlassian/conflue
root      599854  1.0  1.3 7007820 427956 pts/0  Sl+  Nov20  28:11      |   \_ /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java -classpath /opt/atlassian/conf
root      701694  0.0  0.0   4288   764 ?        Ss+  Nov20   0:00      \_ /bin/sh
```

Преимущество #2: Простота микросервисов

SOC FORUM 2023

- Микросервис проще ОС и монолитов
  - Наличие небольшой, выделенной логики
  - Малое количество процессов
  - Часто stateless



Преимущество #3: Работа микросервисов в несколько копий/реплик

SOC FORUM 2023

The Defender's Advantage at Scale

- Attackers can't attack all targets at once, any successful attack with side-effects will be an outlier
- Side-effects aren't always obvious to attackers
- The more replicas, the more anomalous outliers look
- Applies to production servers and endpoint software
- Anomaly detect all the things and find the outliers!

"Thinking Outside the Box: Or, How I Learned to Stop Worrying and Love the Cloud", Dino A. Dai Zovi

Преимущество #4: Kubernetes это декларативная система

SOC FORUM 2023

- Все что касается Kubernetes Resources идет через Kubernetes API server
  - “Все” есть YAML
  - “Все” можно изменять и валидировать до момента применения в кластере
  - “Все” попадает в Kubernetes Audit Log
    - Исключение интерактивные команды, прямые обращения а kubelet API и runtime
      - Kubectl exec – установленное соединение по WebSocket
      - Нужен Runtime агент
- Компании все чаще идут к концепции Everything-as-Code к GitOps
  - Infrastructure-as-Code
  - Configuration-as-Code
  - Policy-as-Code
  - Security-as-Code
  - …

Заключение

Необходимо понимать контейнеры, Kubernetes и то окружение за которое вы отвечаете

Необходимо фиксировать инциденты в контейнерах максимально быстро пока они еще существуют

SOC FORUM 2023

Необходимо использовать иммутабельность, распределенность и эфемерность контейнерных инфраструктур в свою пользу

Лучше/проще/дешевле не доводить до инцидентов в контейнерах, но это другая история ;)

Спасибо за внимание!

SOC FORUM 2023

LUNTRY

Дмитрий Евдокимов
Founder&CTO

Email: de@luntry.ru
Twitter: @evdokimovds
@Qu3b3c
Channel: @k8security
Site: www.luntry.ru

SOC FORUM 2023