Aramis

Présentation du 05 juin 2025

Sensibilisation, Formation, Evénements

FR - 2025

QUI SOMMES NOUS ? 1/2

Notre histoire

Née de l'association Root-Me, Root-Me PRO a été créée en 2019 pour répondre aux enjeux spécifiques des professionnels (écoles, administrations, entreprises…). Les deux entités œuvrent aujourd'hui en synergie pour un maximum d'impact.

CONTENUS DÉDIÉS AUX PARTICULIERS

Association Root-Me

La plus grande communauté cyber francophone
+ 750 000 membres
+ 18 ans d'existence
+ 1 million de pages vues /mois

CONTENUS DÉDIÉS AUX PROFESSIONNELS

Root-Me PRO

Sensibilisation aux risques numériques
Promotion de la filière cyber
Orientation vers les différents métiers
Formation active via des épreuves réalistes

IMPACTS SUR L'ÉCOSYSTEME CYBER

- Attractivité renforcée du secteur
- Emergence de nouveaux talents
- Développement des compétences cyber
- Résilience augmentée face aux menaces

QUI SOMMES NOUS ? 2/2

Nos actions, nos engagements

Root-Me PRO propose des contenus pratiques (challenges, fiches synthèse, vidéos…) combinant une approche ludique, réaliste et pragmatique pour répondre à des besoins variés autour des thématiques suivantes :

SENSIBILISATION AUX RISQUES

AIDE À L'ORIENTATION

ÉVALUATION DES COMPÉTENCES

FORMATION TECHNIQUE

ÉVÉNEMENTS

Ateliers pratiques , démonstrations, compétitions (CTFs), escapes games, conférences…

Événements à portée régionale, nationale ou internationale

Root-Me PRO a été choisie pour faire partie du Consortium créé à l'initiative du Campus Cyber dans le cadre du projet « TalCyb – Talents Cyber ».

Objectif du projet : contribuer à palier la pénurie de talents dans le secteur de la cybersécurité.

CAMPUS CYBER

FRANCE 2030

ILS NOUS FONT CONFIANCE

EDUCATION

PROS / INSTITUTIONNELS

ILS PARLENT DE NOUS

aeif

“La plateforme Root-Me PRO permet aux professeurs de proposer des parcours ciblés de différents niveaux aux élèves. Le suivi personnalisé de la progression de chacun des élèves est très agréable.
Elle offre également des documents pédagogiques associés et des propositions de solutions des challenges (uniquement pour les professeurs).”

-AEIF-

Lycée polyvalent Jean Jaurès – académie Montpellier

“Ce que mes élèves ont aimé dans Root-Me PRO c’est le côté défi et joueur. Pour les plus en difficulté, les premiers challenges réussis ont permis de décoincer leur vision de l’informatique comme matière austère et difficile. Pour les autres, cela a crée des vocations, ou parfois simplement approfondi leurs connaissances sous un jour nouveau.

Outre la vision ludique, ce que j’ai apprécié chez Root-Me PRO, en tant que professeur d’informatique, c’est une vision différente, plus ancrée dans le réel et l’usage de certaines notions du programme qui sinon restent très théoriques. Par ailleurs les challenges plus avancés donnent une vision très complémentaire des notions enseignées au lycée. Et j’ai appris beaucoup de choses !”

Frédéric MANDON - Professeur d’informatique au Lycée Jean Jaurès Saint-Clément-de-Rivière - www.maths-info-lycee.fr

Aurélien
Cybersecurity engineer apprentice
1 an(s) •

C'est la fin de ma toute première compétition de hacking.
J'en sors avec un mélange de bonheur, de fatigue et de frustration. C'est vraiment incroyable comme sensations, on passe par toutes les émotions dans ce genre de moments.
Je suis frustré parce que je pense que j'aurais pu faire mieux de manière individuelle, mais je vais remédier à ça en travaillant plus 💪
Je suis fatigué parce que mon cerveau a été mis à rude épreuve !
Mais surtout, je suis heureux parce que j'ai appris. Je suis heureux parce j'ai partagé des bons moments avec mes coéquipiers talentueux de la Cybersecurity School. Je suis heureux parce que ça confirme que la cybersécurité est ma passion avant d'être mon métier (même si je dois avouer que l'idée de claquer la porte et d'aller élever des chèvres dans le Larzac m'a traversé l'esprit plusieurs fois aujourd'hui 😅).
Merci à Root-Me PRO et Airbus pour cette incroyable organisation !
Merci à Paul, Daniel, Matias et Max pour cette belle 10e place sur 18, pour une première, on peut être fiers 😊
Et surtout bravo à tous les participants 👏

DGSE - Direction Générale de la Sécurité Extérieure
318 154 abonnés
1 sem. •

[#Evénements]

🚀 J-7 avant le lancement du challenge Root-Me PRO !

Découvrons dès maintenant plus de détails sur la mission qui vous attend !
Merci à Root-Me PRO pour la création de ce défi 💪

Pascale ROUSSET • 1er
Cyber Security Risk & transformation ManagerAirbus | Certified ISO 27005 | E...
1 an(s) •

Root-Me PRO Good Team & Great Job! You Rock!

David Roumanet • 1er
Ingénieur de l'Éducation Nationale (prof quoi 😅)
maintenant •

Root-Me PRO est la société montante du secteur de la cybersécurité. Je suis fier d'avoir été le premier à croire en eux, pour le Réseau Certa.

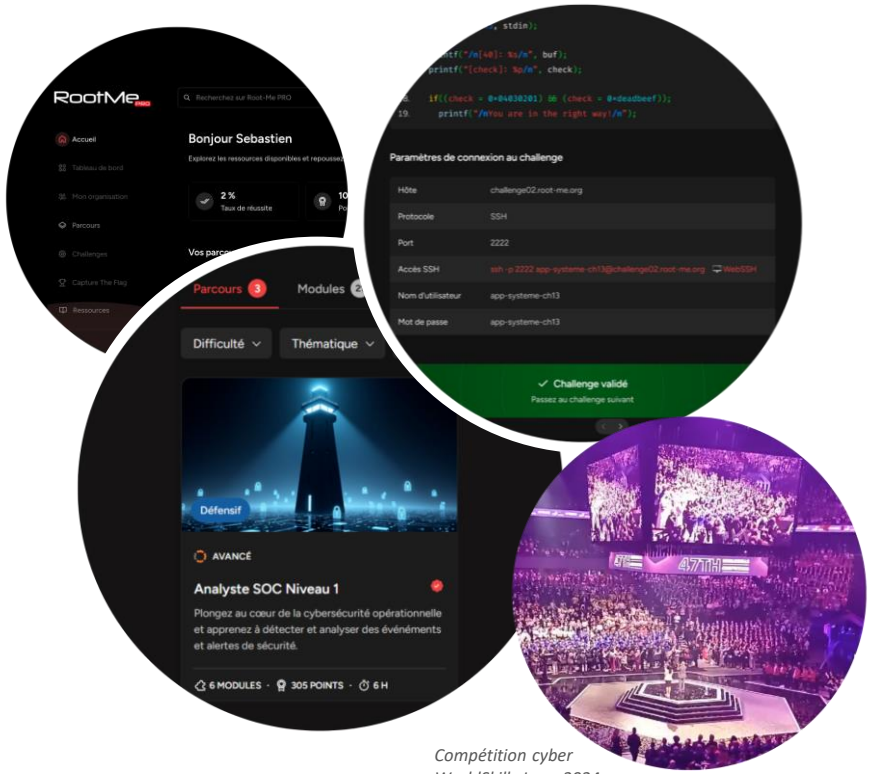
Sylvie G. • 2e
Directrice Adjointe (

Un grand Merci Root-Me PRO pour cette belle opportunité offerte aux étudiants #bts #sio Groupe Saint Jean #rennes

LEMONDE INFORMATIQUE

Intégrer les équipes de cyber spécialistes du ministère des Armées en participant à un concours de hack. C'est l'objectif d'un challenge de type capture the flag (CTF) créé par la plateforme Root-me pro pour le commandement de la cyberdéfense (Comcyber) Cette compétition s'inscrit dans le cadre d'une campagne lancée par l'organisme pour recruter des sous-officiers cyber à l'armée de Terre. D'une complexité intermédiaire, elle s'adresse principalement aux diplômés d'un bac+2 en cybersécurité. Sont concernés des titulaires d'un BTS Ciel (cybersécurité, informatique et réseaux, électronique), SIO (services informatiques aux organisations) ou d'une autre formation de niveau Bac +2 dans l'informatique. Leur mission ? Résoudre une série de défis techniques, soit un total de 6 flags en se glissant dans la peu d'un cybercombattant.

NOS OFFRES



Compétition cyber WorldSkills Lyon 2024

Nos offres répondent à de nombreux cas d'usage en matière de cybersécurité : faire monter vos équipes en compétence, sensibiliser aux risques numériques, renforcer la cohésion, évaluer ou recruter de nouveaux talents…

Nous construisons avec vous des dispositifs sur mesure.

TRAIN MY TEAM

Sur abonnement

- Cas d'usages variés : formations, événements, recrutement…
- Des parcours officiels pour tous les niveaux
- Des centaines de contenus exclusifs : challenges, ressources, vidéos…
- Différents profils utilisateurs : superviseur, formateur, joueur
- Une équipe d'experts passionnés (support, suivi, formation…)

CHALLENGE MY TEAM

Ponctuel

- Cas d'usages variés : CTF, ateliers pratiques, formations ponctuelles, évaluations techniques, sensibilisation, escape games…
- Création et sélection d'épreuves
- Accompagnement tout au long de votre événement : organisation, support, animation, communication

LES BÉNÉFICES

Collaborateur

- Se sensibiliser à la cybersécurité (profils non techniques)
- Perfectionner ses compétences en cybersécurité (profils techniques)
- Se mesurer à ses collègues autour de challenges réalistes

Managers

- Développer les expertises techniques des collaborateurs
- Simplifier la gestion des compétences de ses équipes
- Suivre et comparer leur progression technique

Ressources humaines

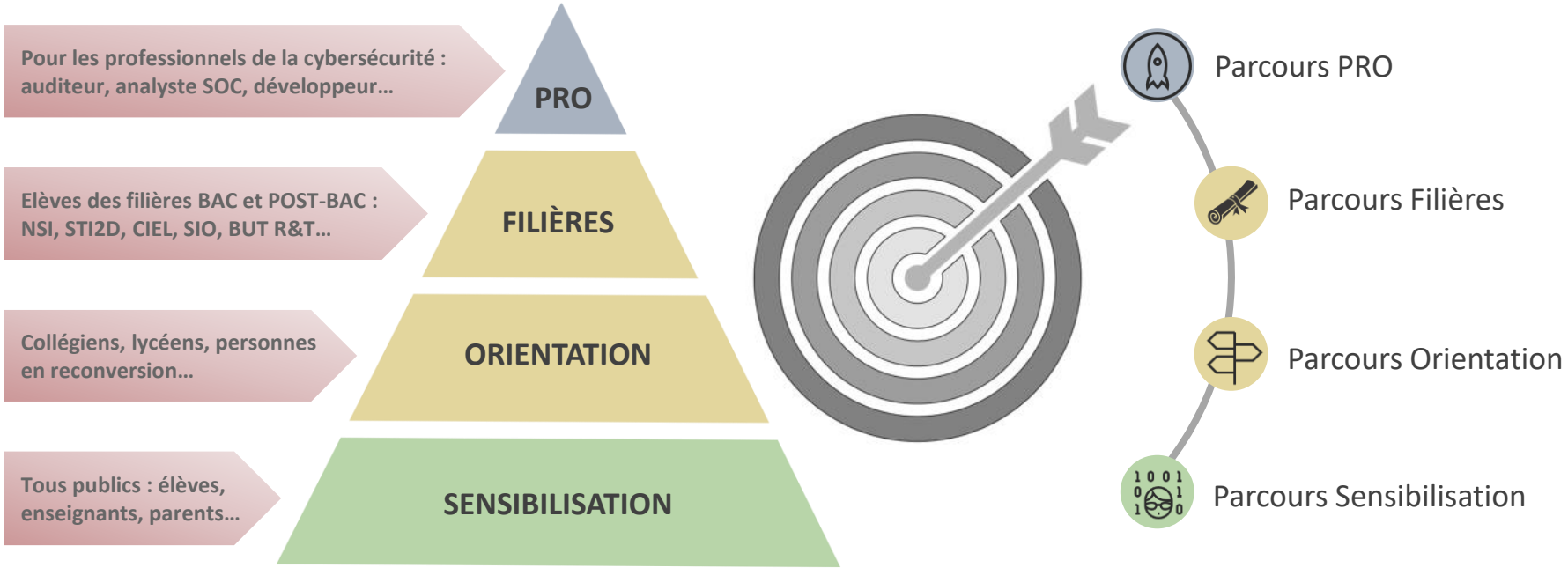
- Identifier les talents émergents et favoriser leur engagement
- Simplifier l'évaluation des compétences techniques
- Accompagner la stratégie d'évolution des collaborateurs

Communication

- Fédérer les équipes au travers d'événements ludiques
- Renforcer l'image de marque auprès de la communauté cyber
- Promouvoir ses métiers et ses savoir-faire

NOS PARCOURS & FORMATIONS 1/2

Les parcours officiels de Root-Me PRO sont adaptés à chaque niveau, de la **sensibilisation aux risques** numériques jusqu'à la **formation avancée** pour les professionnels désireux d'approfondir leurs compétences cyber selon leur métier.



NOS PARCOURS & FORMATIONS 2/2

PARCOURS SENSIBILISATION

Accessible à tous, ce parcours vise **à sensibiliser aux risques** liés au numérique. À travers différents scénarios réalistes, les participants découvrent les méthodes utilisées par les attaquants et intègrent les **meilleures pratiques** pour se protéger plus efficacement.

PARCOURS ORIENTATION

Destiné aux collégiens, lycéens et personnes en reconversion, ce parcours permet de **découvrir différents métiers de la cybersécurité**. Les challenges proposés couvrent des **domaines variés** comme la sécurité du web, des réseaux, des systèmes…

PARCOURS FILIERES

Destinés aux élèves engagés dans les **filières BAC et POST-BAC (SIO, STI2D, CIEL, NSI…),** ces parcours ont été conçus et testés avec les enseignants référents de chaque filière. Adaptés à chaque filière, ils incluent des ressources variées (challenges, fiches, vidéos…).

PARCOURS PRO

Conçus pour les professionnels souhaitant **renforcer ou actualiser** leurs compétences en cybersécurité, ces parcours couvrent les **besoins spécifiques de métiers variés** : pentester (auditeur), analyste SOC, développeur, administrateur, ingénieur IA, etc.

EXEMPLES DE RÉALISATIONS 1/3

FORMATIONS

Sensibiliser, orienter, former, spécialiser…

OPENCLASSROOMS

Co-création de programmes de **formation en ligne** alliant projets concrets, accompagnement personnalisé et accès à un **environnement dédié Root-Me PRO**.

Exemples de formations : réaliser un test d'intrusion web, sécuriser son Active Directory, boot camp cyber…

e-santé GRADeS Pays de la Loire

e-santé Occitanie Connecter pour mieux soigner

GROUPEMENT RÉGIONAL e-santé BRETAGNE

esea LA E-SANTÉ NOUVELLE-AQUITAINE

GCSoara la santé connectée

Formations opérationnelles dispensées dans le cadre du **programme CaRE** pour les équipes informatiques et sécurité **d'établissements de santé** (CH, CHU, GHT, EMS…), en lien avec les Groupements Régionaux d'Appui à la e-Santé (GRADeS).

Création et mise à disposition de **lab Active Directory** sur les environnements Root-Me PRO.

Thématiques :
Sécurisation de l'Active Directory Niveau 1 & 2, Sécurisation des sauvegardes, Supervision de sécurité

+ de 250 personnes formées depuis 2024

Création d'un parcours personnalisé pour la formation "**Assistant(e) en cybersécurité**".

CNED CONNECTÉ À VOTRE AVENIR

Composé de **8 modules** et de **dizaines de challenges**, ce parcours couvre des domaines variés allant de la **sécurité offensive** à la **sécurité défensive**.

Accessible en ligne et en asynchrone, la formation peut être suivie sur 18 mois et s'adapte aux contraintes des personnes en poste, aux personnes en reconversion ou en recherche d'emploi, en leur offrant une spécialisation valorisante sur un marché en tension.

EXEMPLES DE RÉALISATIONS 2/3

ÉVÉNEMENTS

Challenger, fidéliser, attirer, recruter…

AIRBUS

Co-organisation et création des épreuves techniques (challenges, escape game) pour la **compétition annuelle de cybersécurité dédiée aux équipes IT et sécurité de l'ensemble des entités monde du Groupe Airbus (+300 participants).**

Finale internationale WorldSkills Lyon 2024

Création des épreuves de la compétition cybersécurité :

- Épreuve Red Team (Pentest web/AD…)
- Épreuve Blue Team (SOC/Forensic)

Pendant les 4 jours de compétition, animation d'ateliers pratiques pour des milliers de visiteurs en quête d'information et de découvertes : challenges, présentation des métiers de la cybersécurité, sensibilisation aux risques…

Création des épreuves de sélection des équipes régionales pour la **compétition nationale** qui se déroulera à Marseille en octobre 2025.

IN CYBER FORUM EUROPE

Création de l'épreuve **Active Directory** (11 flags, 2 machines) pour l'**European Cyber Cup 2025**, la compétition annuelle du **Forum INCYBER (FIC).**

Création du **CTF HACK'N GAME,** événement de type Capture The Flag dédié aux élèves des filières professionnelles CIEL et SIO.

*Finale organisée en partenariat avec le **Campus Cyber** dans le cadre du **Festival des Hauts de Seine Digital Games.***

EXEMPLES DE RÉALISATIONS 3/3

SUR MESURE

Communiquer, innover, rayonner, attirer

Des formats innovants pour des cas d'usage variés : susciter des vocations, évaluer des compétences, détecter de nouveaux talents, rayonner et développer son image de marque...

Création d'un **challenge réaliste,** sur demande du **Commandement de la cyberdéfense,** au profit de la **Marine nationale**.

Composé de 6 étapes, ce challenge illustre la variété des missions des sous-officiers mariniers spécialisés en cyberdéfense. L'objectif ? Mener une enquête suite à la détection d'un drone survolant un navire militaire.

Ce challenge a permis aux participants de tester leurs compétences sur des scénarios inspirés du terrain.

Il a également permis à la Marine nationale de faire connaitre ses métiers cyber à des milliers de personnes.

Notre dernière création a été réalisée au profit de la **Direction Générale de la Sécurité extérieure (DGSE)**.

Ce challenge réaliste, composé de 6 missions variées (web, réseau, forensic, android…) s'adresse aux passionnés de cybersécurité curieux de découvrir les missions et les opportunités de carrière dans le domaine du renseignement. Une expérience immersive qui a conquis déjà des centaines de participants !

Challenge ouvert
jusqu'au 7 mai 2025

dgse.pro.root-e.org/

L’environnement

Les principaux challenges d'architecture

Isolation des environnements : empêcher les utilisateurs d'échapper aux machines vulnérables et d'atteindre l'infrastructure sous-jacente.

Gestion de la persistance et du reset : assurer que chaque machine / challenge revienne à son état initial vulnérable, tout en empêchant la compromission persistante.

Séparation entre infrastructure et labs : empêcher les utilisateurs d'atteindre l'infrastructure réelle (portail web, base de données utilisateurs, API, backend admin, etc.).

Détection et prévention des abus : les utilisateurs peuvent tenter de dépasser les limites (DoS, brute force, enumeration massive, scan inter-labs, etc.).

Protection des comptes et des données utilisateur : empêcher les attaques internes ou externes visant à voler des credentials, des flags, ou du contenu privé.

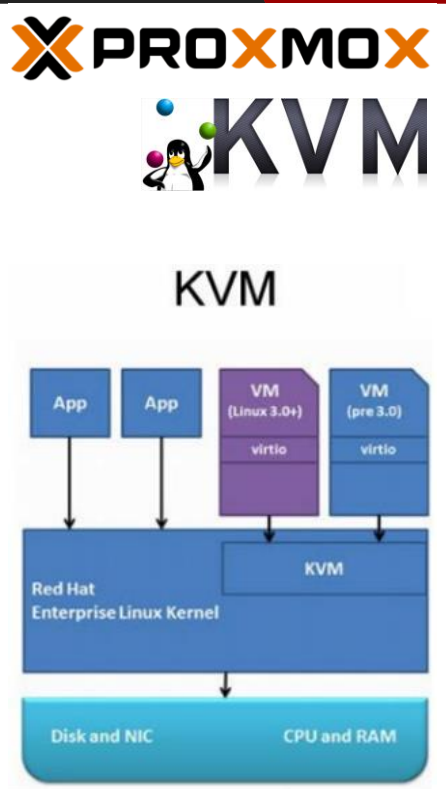
Sécurisation des interfaces : les interfaces web et APIs peuvent être attaquées (injections, auth bypass, RCE via uploads, etc.).

Scalabilité, Disponibilité, protection contre les fuites de flag / cheat, gestion des vulnérabilités internes…..

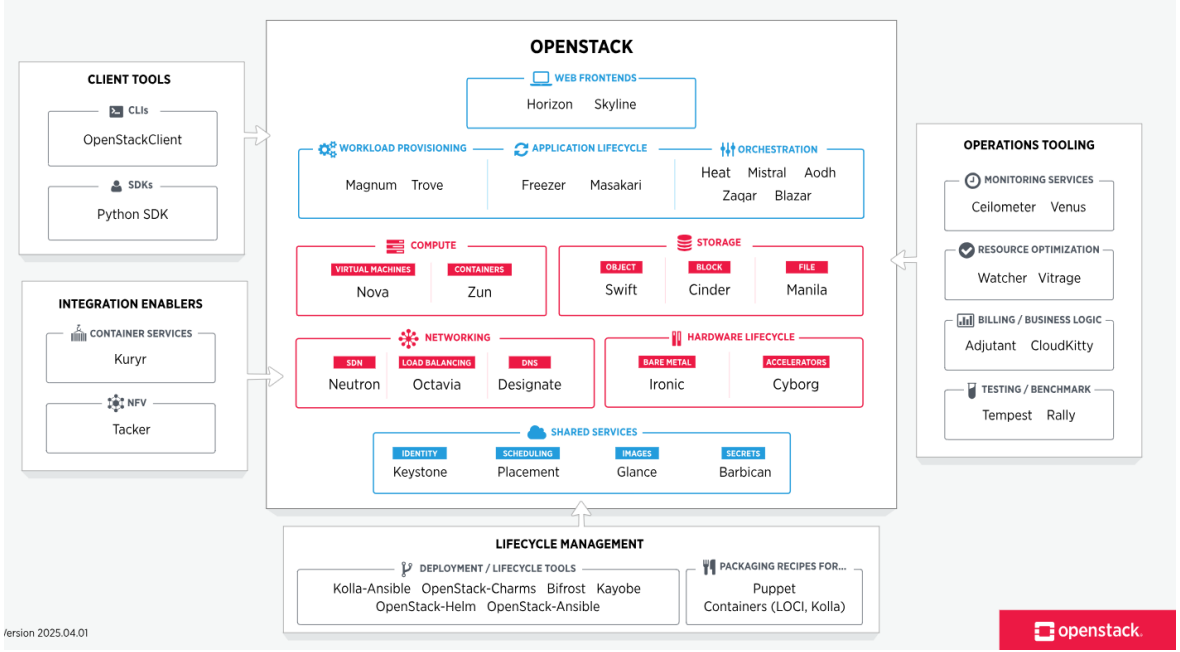
Un peu d'open dans votre souveraineté ?

Le cloud

- KVM (Kernel-based Virtual Machine) est une technologie de virtualisation complète intégrée directement dans le noyau Linux. Introduit en 2007 et officiellement intégré au noyau Linux à partir de la version 2.6.20, KVM transforme Linux en un hyperviseur de type 1, permettant aux utilisateurs d'exécuter plusieurs machines virtuelles (VM) sur un seul hôte physique.
- KVM s'appuie sur QEMU (Quick EMUlator) pour l'émulation des périphériques et la gestion des images disque, tandis que le module KVM lui-même s'occupe de la gestion des processeurs virtuels et de la mémoire. Cela permet à KVM de prendre en charge de nombreux systèmes d'exploitation invités, notamment Linux, Windows, BSD et d'autres OS compatibles x86.
- Les pilotes VirtIO sont des périphériques paravirtualisés qui permettent aux VMs d'accéder aux ressources matérielles de manière quasi-native. Ils remplacent l'émulation de QEMU par une interface plus directe et optimisée.

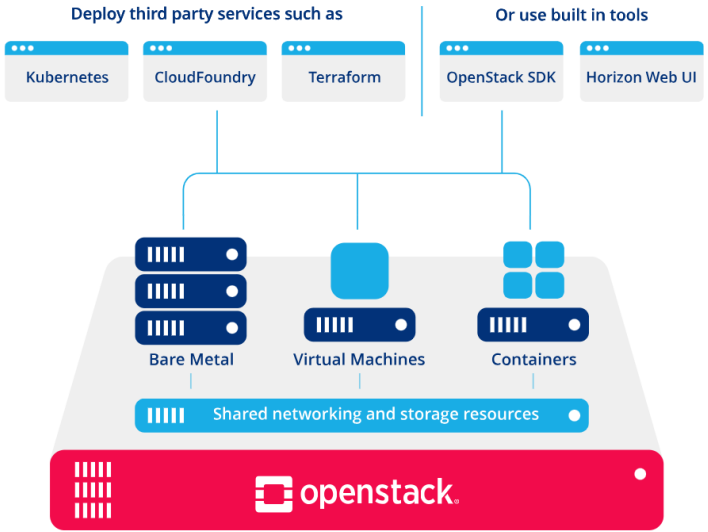


Le cloud



openstack.

An OpenInfra Foundation Project



Le cloud

Platinum (12)

ERICSSON FUJITSU HITACHI HUAWEI intel Meta Microsoft

NEC ORACLE QUALCOMM IBM Red Hat SAMSUNG

kubernetes

CLOUD NATIVE COMPUTING FOUNDATION

THE LINUX FOUNDATION

Gold (14)

Baidu 百度 cisco DELL Technologies FUTUREWEI Technologies Google HONDA The Power of Dreams LY Corporation

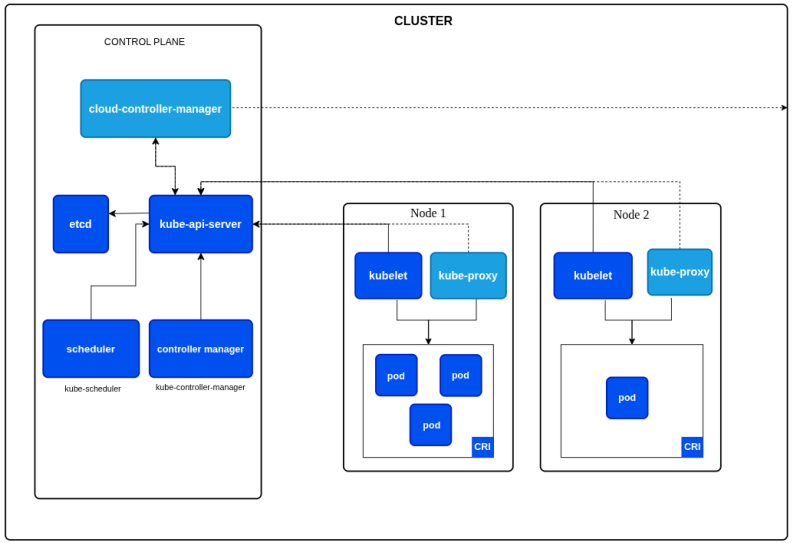
MITSUBISHI ELECTRIC Panasonic AUTOMOTIVE Panasonic RENESAS SONY TOSHIBA TOYOTA

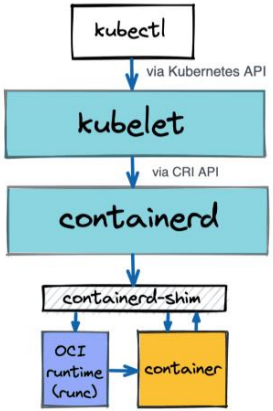
Fermer cette boîte de dialogue

Silver (1311)

PS CLOUD SERVICES 1NCE 1Nebula 1Password 23 Technologies GEEKS SOLUTIONS 2bcloud

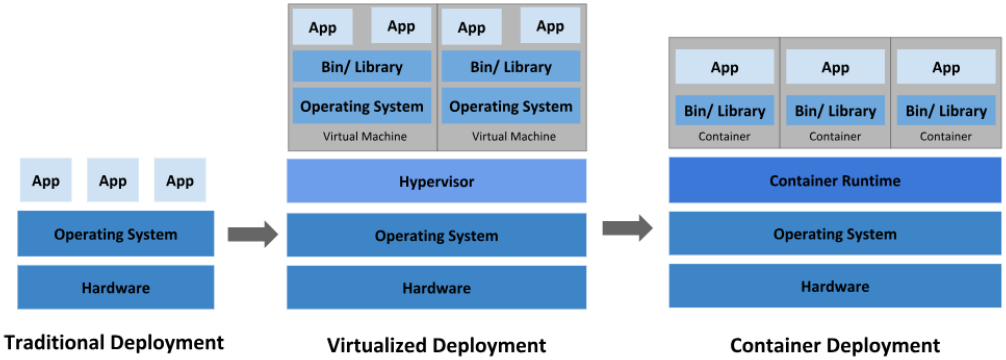
Le cloud



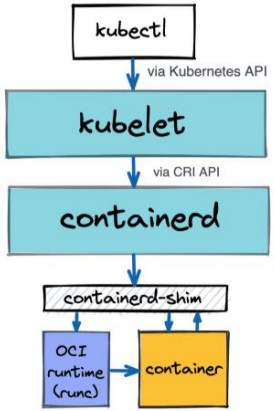


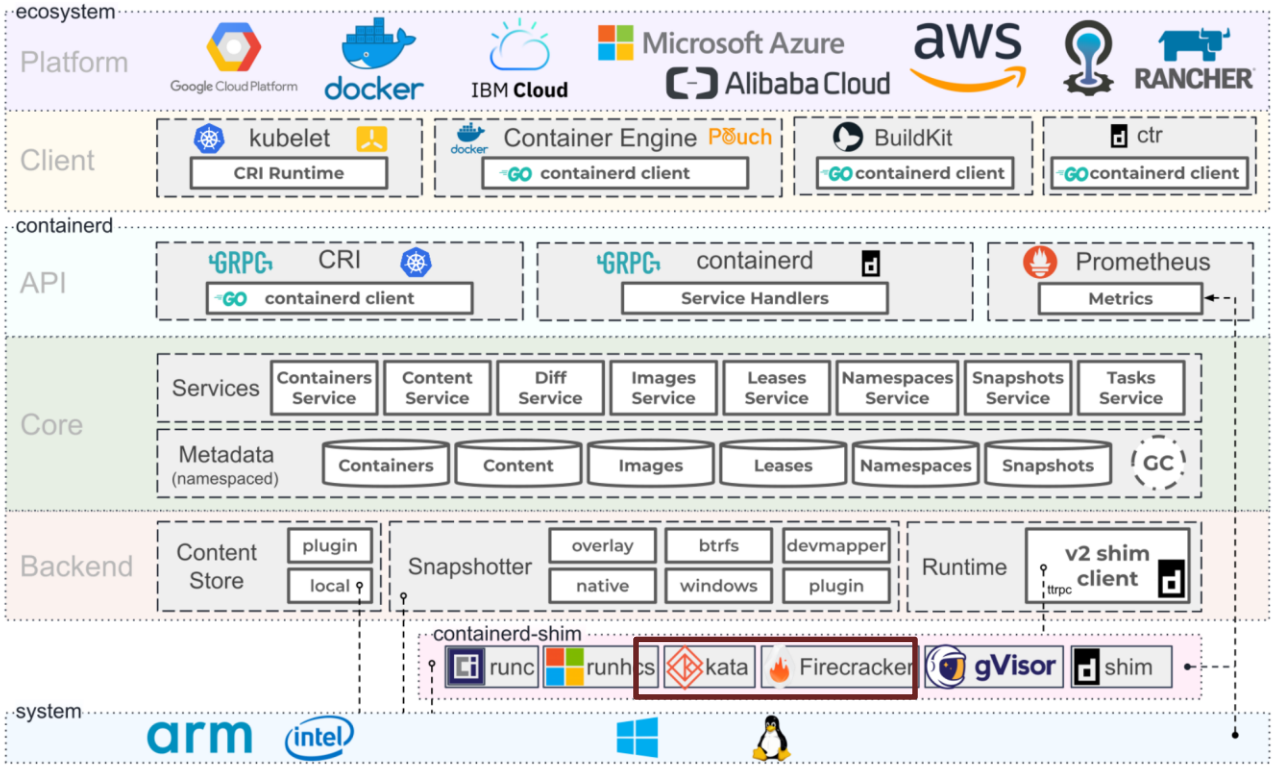
kubernetes

CLOUD NATIVE COMPUTING FOUNDATION



Le cloud



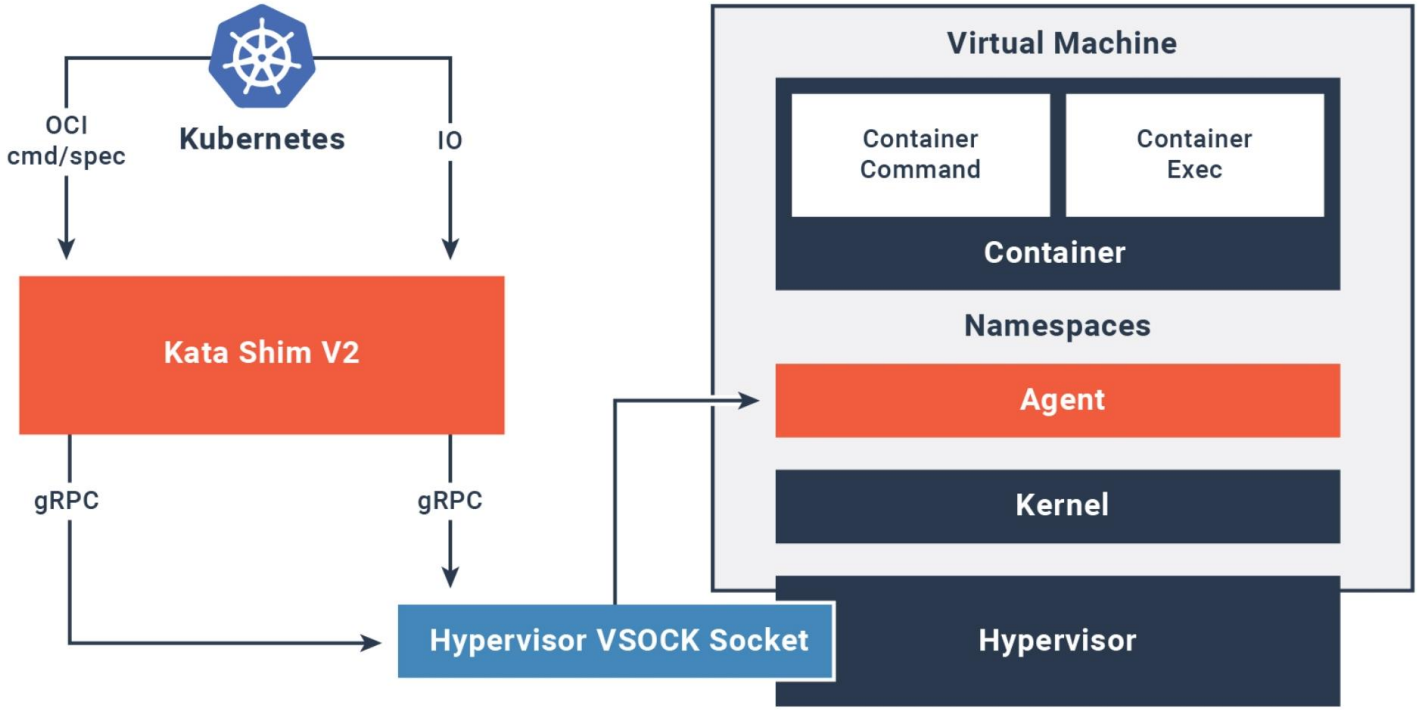


kubernetes

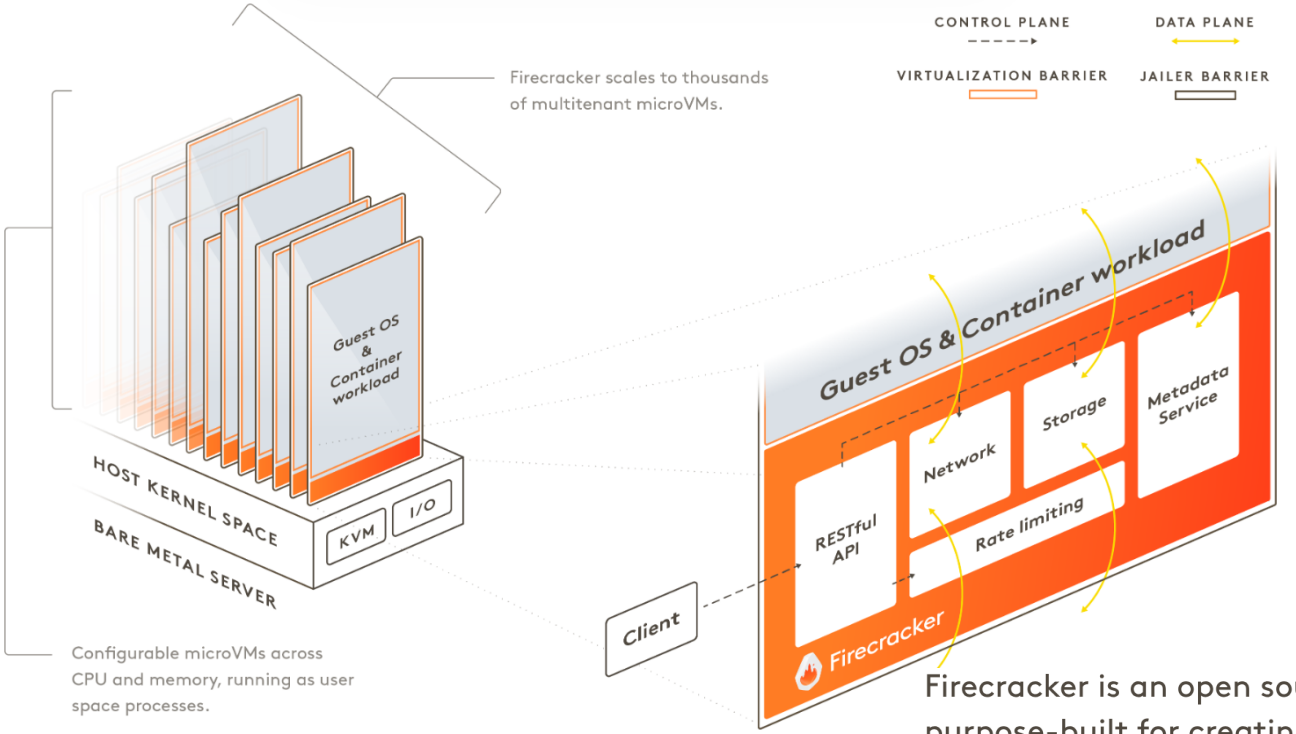
CLOUD NATIVE COMPUTING FOUNDATION

containerd

Le cloud



Le cloud



Firecracker is an open source virtualization technology that is purpose-built for creating and managing secure, multi-tenant container and function-based services.

Le cloud

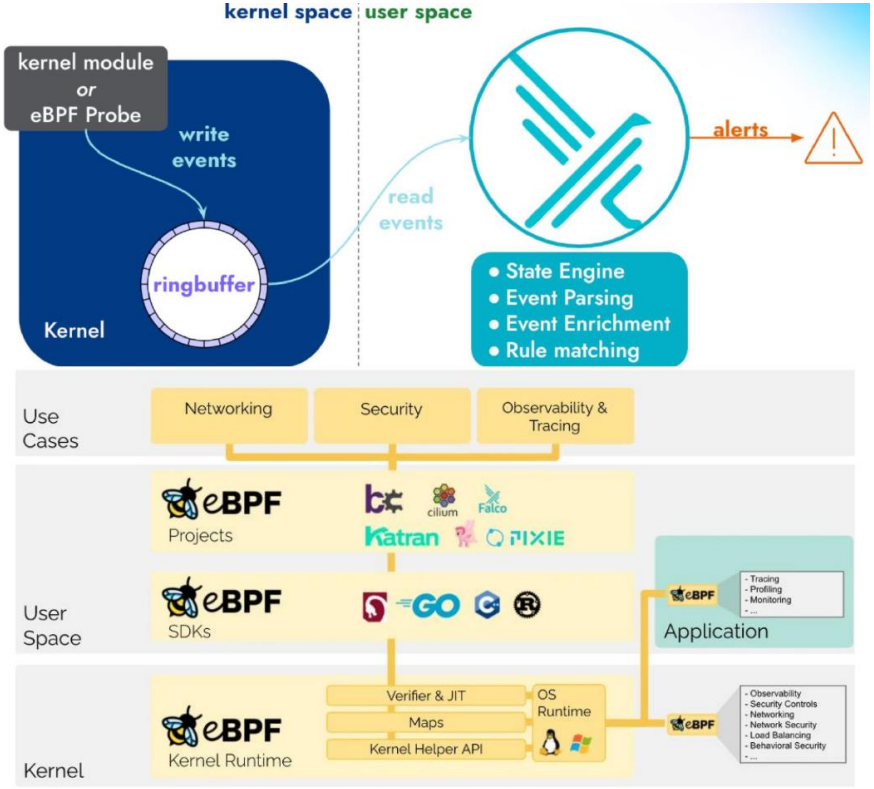
- Grype : A vulnerability scanner for container images and filesystems. Easily install the binary to try it out. Works with Syft, the powerful SBOM (software bill of materials) tool for container images and filesystems.
- Syft : A CLI tool and Go library for generating a Software Bill of Materials (SBOM) from container images and filesystems. Exceptional for vulnerability detection when used with a scanner like Grype.


```
~/code/grype main                                                    01:21:52 PM
py382 ❯ grype clashapp/qa-page | head
 ✔ Vulnerability DB        [no update available]
 ✔ Pulled image
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged image         [113 packages]
 ✔ Scanned image           [248 vulnerabilities]
NAME                        INSTALLED              VULNERABILITY     SEVERITY
apt                         1.4.10                 CVE-2011-3374     Negligible
bash                        4.4-5                  CVE-2019-18276    Negligible
coreutils                   8.26-3                 CVE-2016-2781     Low
coreutils                   8.26-3                 CVE-2017-18018    Negligible
e2fslibs                    1.43.4-2+deb9u1        CVE-2019-5188     Medium
e2fsprogs                   1.43.4-2+deb9u1        CVE-2019-5188     Medium
gcc-6-base                  6.3.0-18+deb9u1        CVE-2018-12886    Medium
gpgv                        2.1.18-8~deb9u4        CVE-2019-14855    Low
gpgv                        2.1.18-8~deb9u4        CVE-2018-1000858  Medium

~/code/grype main 8s                                                 01:22:09 PM
py382 ❯
```

Le cloud

```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scored)
[FAIL] 1.1.19 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Scored)
[PASS] 1.1.20 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.21 Ensure that the --token-auth-file parameter is not set (Scored)
[FAIL] 1.1.22 Ensure that the --kubelet-certificate-authority argument is set as appropriate (Scored)
```

Le cloud

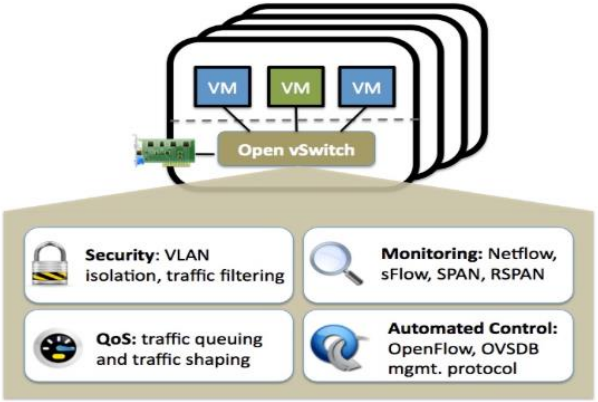


Falco

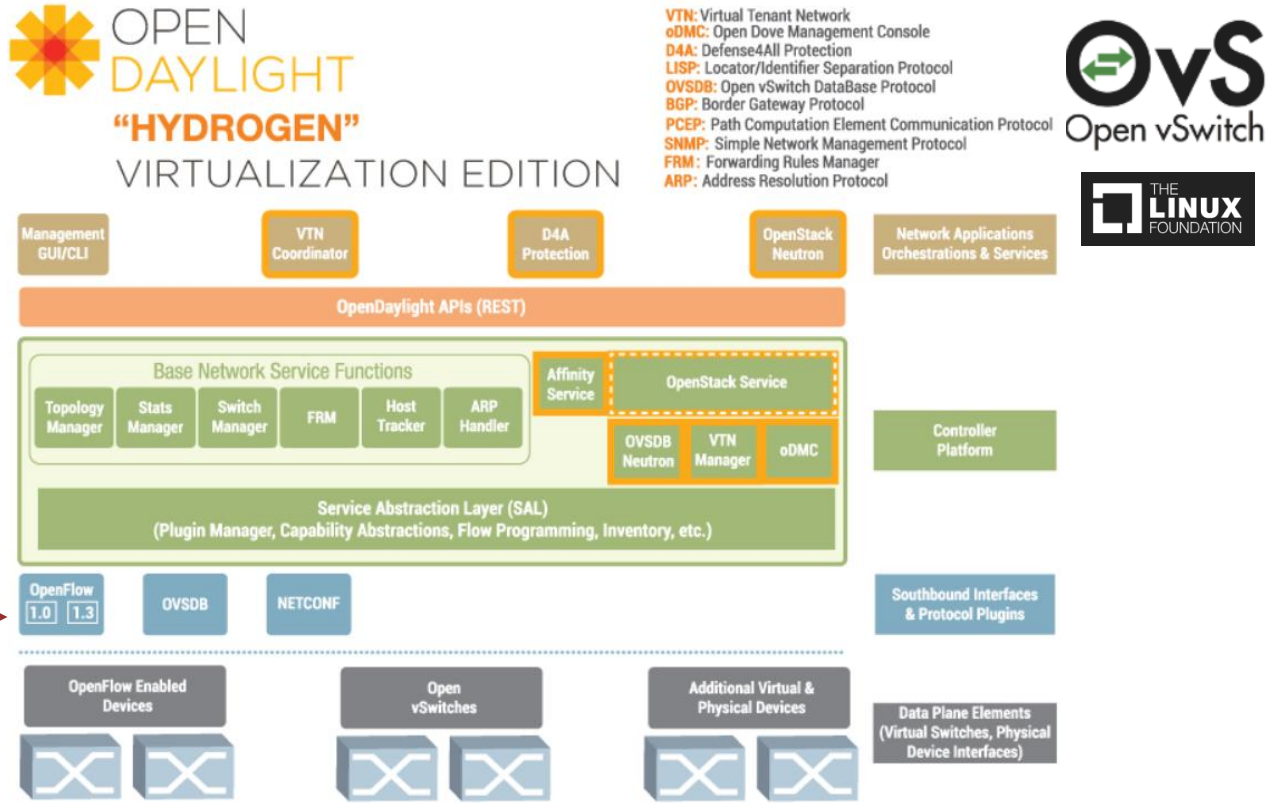
Falco is a cloud-native security tool. It provides near real-time threat detection for cloud, container, and Kubernetes workloads by leveraging runtime insights. Falco can monitor events from various sources, including the Linux kernel, and enrich them with metadata from the Kubernetes API server, container runtime, and more.

Once Falco has received these events, it compares them to a set of rules to determine if the actions being performed need further investigation. If they do, Falco can forward the output to multiple different endpoints either natively (syslog, stdout, HTTPS, and gRPC endpoints) or with the help of Falcosidekick, a companion tool that offers integrations to several different applications and services.

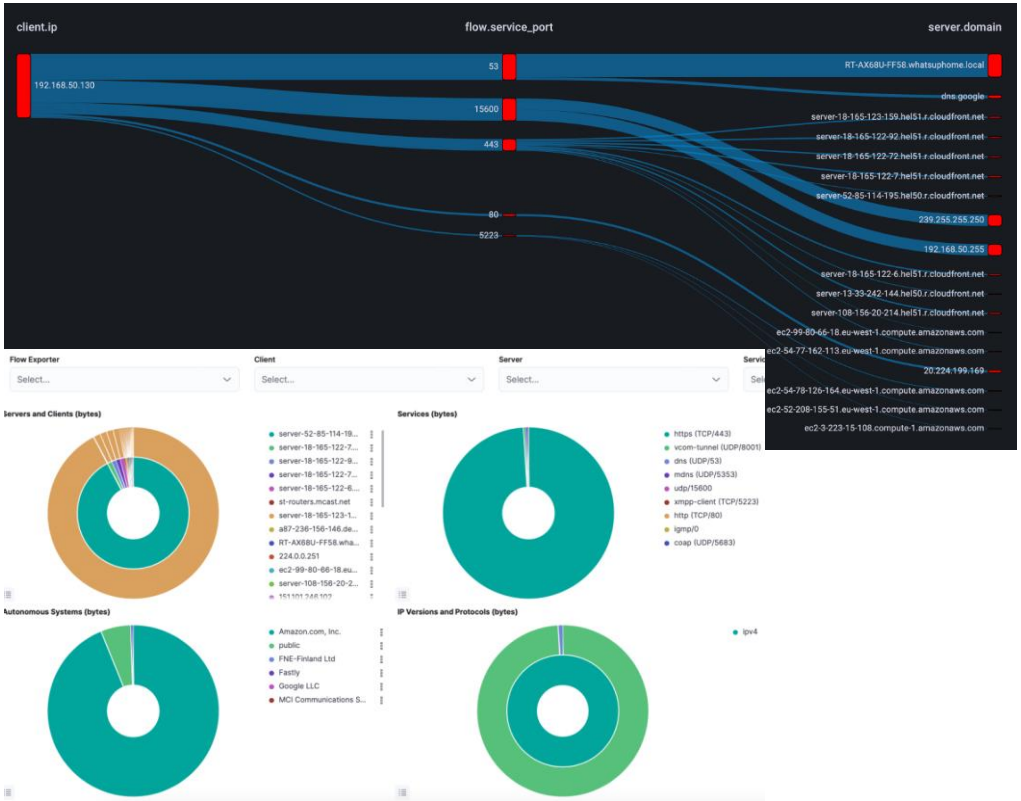
Le cloud



- Bareudp
- Basic Configuration
- Development
- Implementation Details
- General
- Common Configuration Issues
- Using OpenFlow
- Quality of Service (QoS)
- Releases
- Terminology
- VLANs
- VXLANs



Network

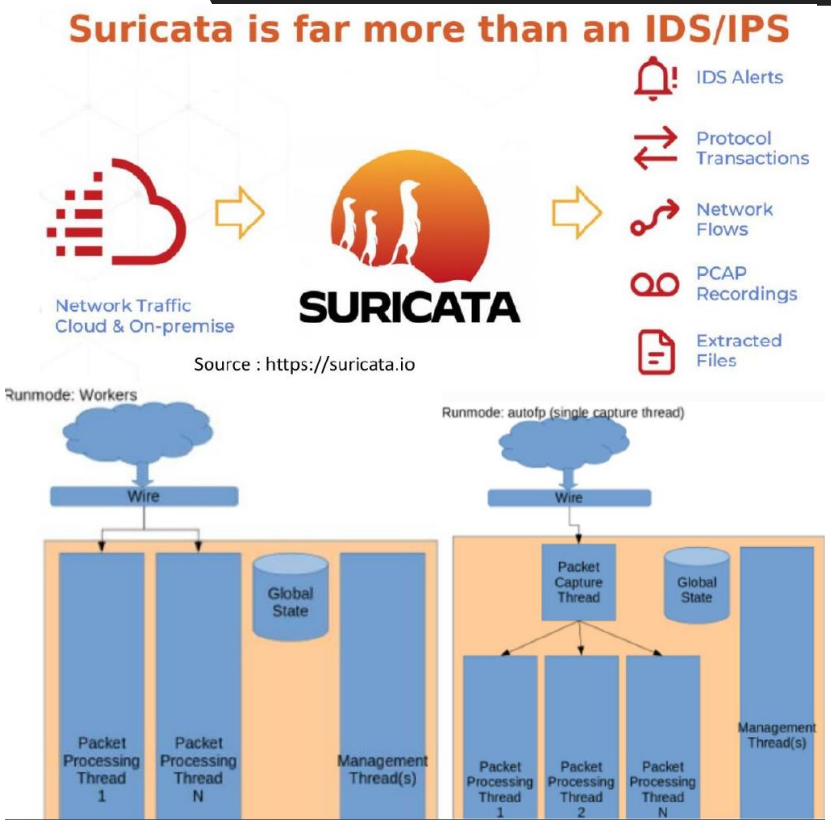


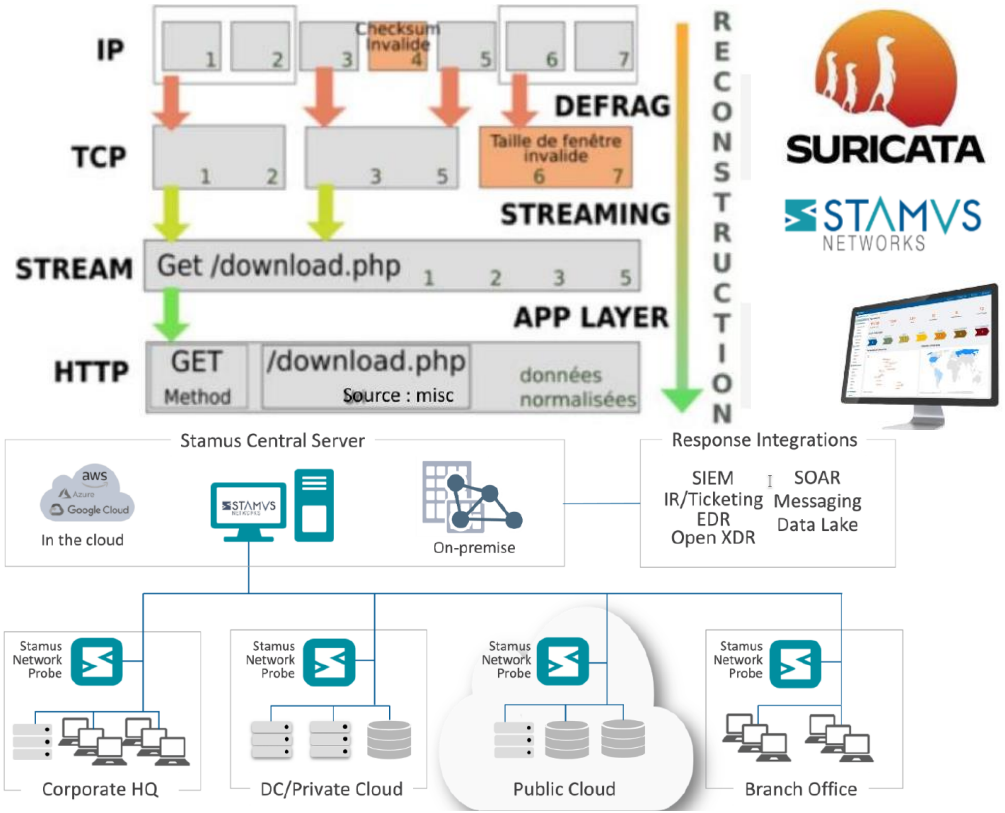
Netflow / IPFIX

elastic

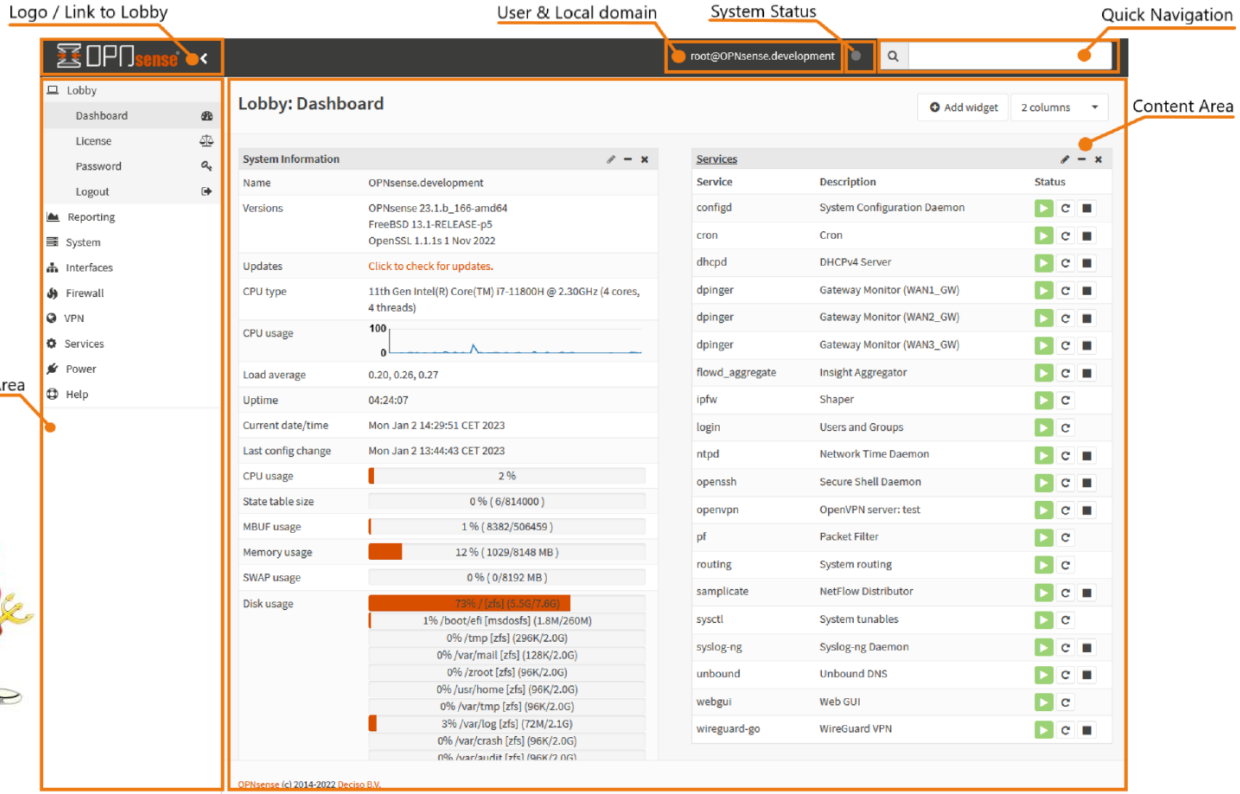
client.domain	Samsung.whatsuphome.local
client.ip	192.168.50.130
client.packets	1
destination.as.organization.name	private
destination.domain	192.168.50.255
destination.ip	192.168.50.255
destination.port	15600
ecs.version	1.5.0
event.category	network
event.dataset	netflow
event.duration	0
event.end	Feb 20, 2023 @ 06:46:03.905
event.kind	event
event.module	flow
event.severity	6
event.start	Feb 20, 2023 @ 06:46:03.905
event.type	connection
flow.direction	ingress

Network





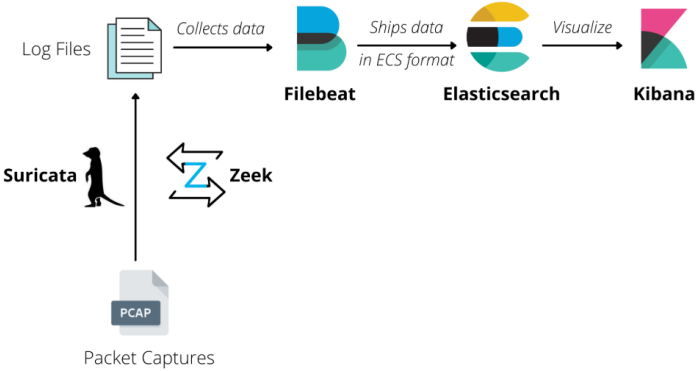
Network

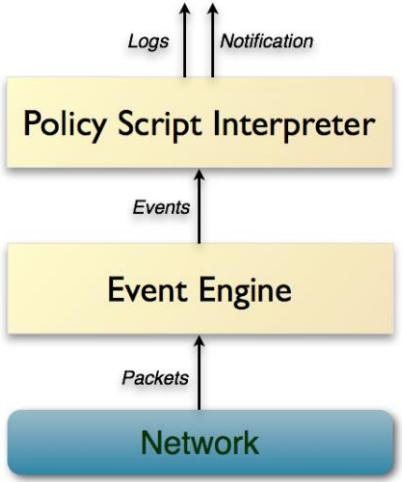


vyos

Network

- **Packet Capture :** récupération des paquets (via libpcap, AF_PACKET, etc.)
- **Event Engine :** analyse des paquets, reconstruction des connexions TCP/UDP
- **Protocol Parsers :** analyse des protocoles : HTTP, DNS, SSL, SMB, FTP, etc.
- **Script Engine** : traitement logique via scripts Zeek (langage Zeek)
- **Loggers :** génère des fichiers .log (conn.log, dns.log, http.log, ssl.log, notice.log, files.log…)
- **Notice Framework :** détection d'événements anormaux, alertes
- **Intel Framework :** corrélation avec IOC (indicateurs de compromission)





Un peu de renforcement ?

Cloud Providers

- Alibaba Cloud
- Amazon Web Services
- Google Cloud Computing Platform
- Google Workspace
- IBM Cloud Foundations
- Microsoft 365
- Microsoft Azure
- Microsoft Dynamics 365 Power Platform
- Oracle Cloud Infrastructure

Desktop Software

- Microsoft Exchange Server
- Microsoft Office
- Zoom
- Google Chrome
- Microsoft Web Browser
- Mozilla Firefox
- Safari Browser

DevSecOps Tools

- Software Supply Chain Security

Mobile Devices

- Apple iOS
- Google Android

Multi Function Print Devices

- Print Devices

Network Devices

- Check Point Firewall
- Cisco
- F5
- Fortinet
- Juniper
- Palo Alto Networks
- pfSense Firewall
- Sophos

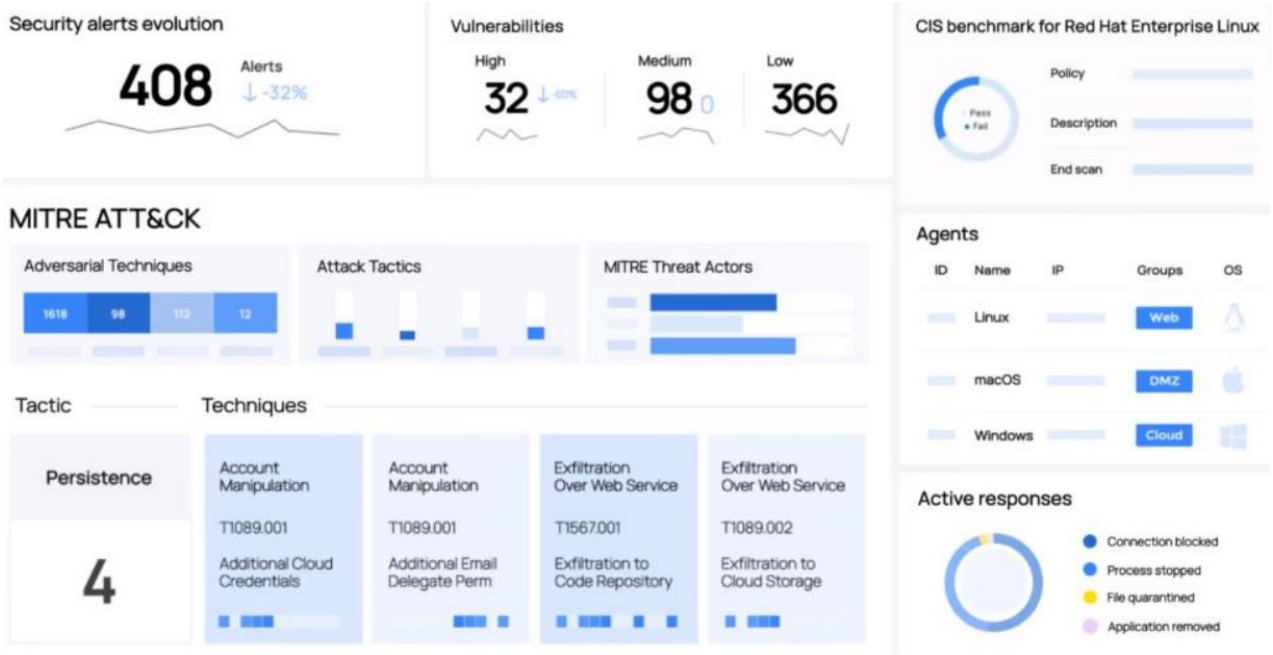
Operating Systems

- IBM i
- IBM Z System
- Aliyun Linux
- AlmaLinux OS
- Amazon Linux
- Bottlerocket
- CentOS Linux
- Debian Family Linux
- Debian Linux
- Distribution Independent Linux
- Fedora Family Linux
- LXD
- Oracle Linux
- Red Hat Enterprise Linux
- Robot Operating System (ROS)
- Rocky Linux
- SUSE Linux Enterprise Server
- Ubuntu Linux
- Microsoft Intune for Windows
- Microsoft Windows Desktop
- Microsoft Windows Server
- Apple macOS
- IBM AIX
- Oracle Solaris

Server Software

- MIT Kerberos
- Microsoft SharePoint
- Apache Cassandra
- IBM Db2
- MariaDB
- Microsoft SQL Server
- MongoDB
- Oracle Database
- Oracle MySQL
- PostgreSQL
- BIND
- Docker
- Kubernetes
- VMware
- Apache HTTP Server
- Apache Tomcat
- IBM WebSphere
- Microsoft IIS
- NGINX

L'HIDS

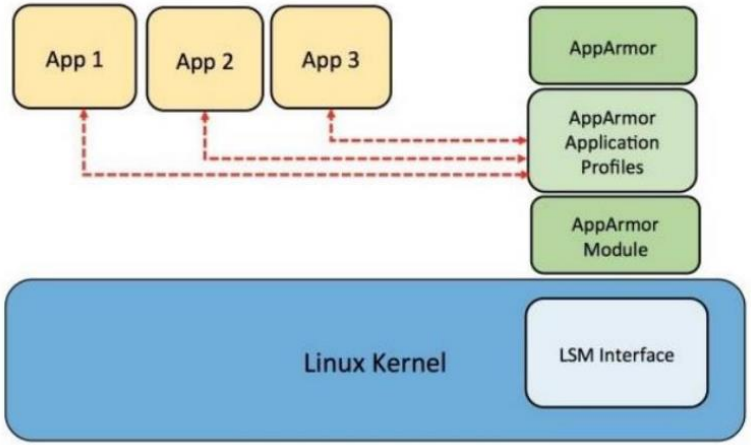


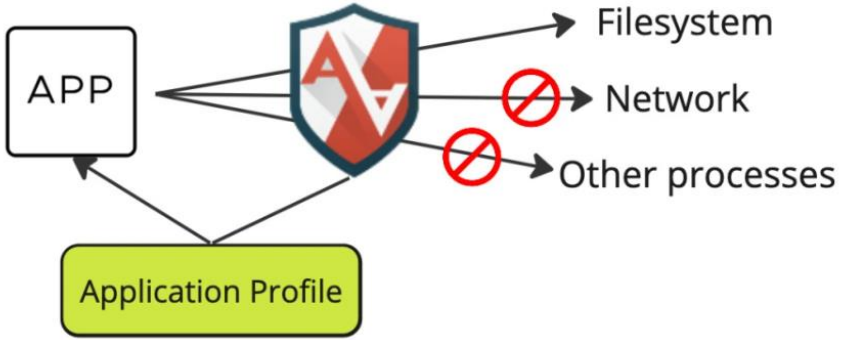
OSSEC wazuh.

- FIM (File Integrity Monitoring)
- Log collection
- Syscheck
- Rootkit detection
- Vulnérabilités
- Command execution
- Découverte, utilisateurs, processus, ports, services etc..

Un peu de renforcement ?

APPARMOR / SELINUX





WAF

Coraza - Web Application Firewall

Regression Tests passing | Coreruleset Compatibility 100% | CodeQL 2 passing | codecov 84% | repo status Active | owasp production project | reference

Coraza is an open source, enterprise-grade, high performance Web Application Firewall (WAF) ready to protect your beloved applications. It is written in Go, supports ModSecurity SecLang rulesets and is 100% compatible with the OWASP Core Rule Set v4.

- Website: https://coraza.io
- Forum: Github Discussions
- OWASP Slack Community (#coraza): https://owasp.org/slack/invite
- Rule testing: Coraza Playground

Integrations

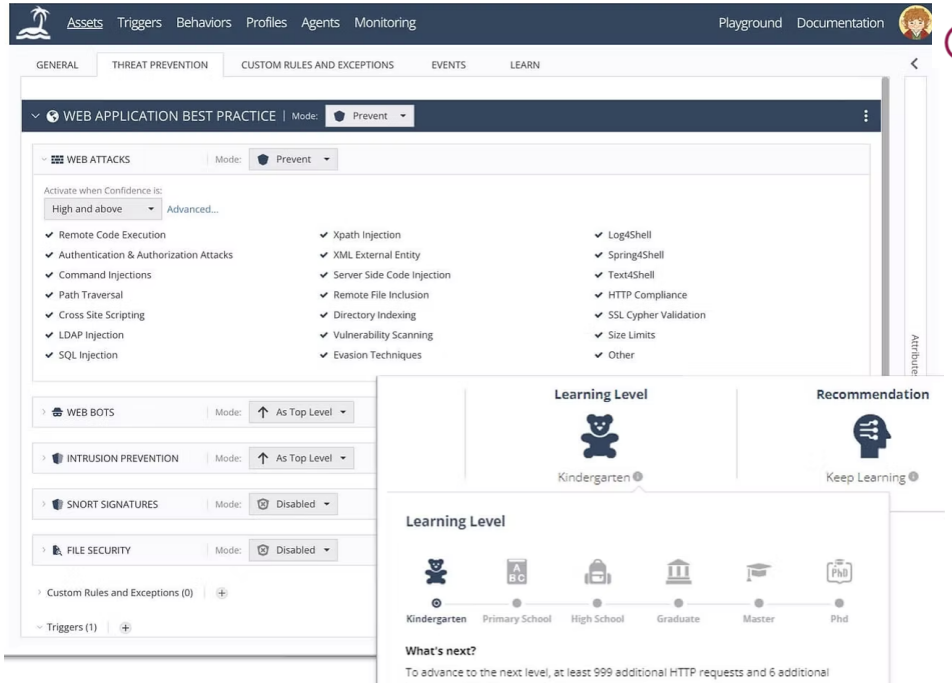
The Coraza Project maintains implementations and plugins for the following servers:

- Caddy Reverse Proxy and Webserver Plugin - stable, needs a maintainer
- Proxy WASM extension for proxies with proxy-wasm support (e.g. Envoy) - stable, still under development
- HAProxy SPOE Plugin - preview
- Traefik Proxy Plugin - preview, needs maintainer
- Gin Web Framework Middleware - preview, needs maintainer
- Apache HTTP Server - experimental
- Nginx - experimental
- Coraza C Library - experimental

Key Features:

- ⇲ **Drop-in** - Coraza is an alternative engine that has partial compatibility with ~~Trustwave~~OWASP ModSecurity Engine and supports industry-standard SecLang rule sets.
- 🔥 **Security** - Coraza runs the OWASP CRS **v4** (Formerly known as Core Rule Set) to protect your web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts. CRS protects from many common attack categories including: SQL Injection (SQLi), Cross Site Scripting (XSS), PHP & Java Code Injection, HTTPoxy, Shellshock, Scripting/Scanner/Bot Detection & Metadata & Error Leakages. Note that older versions of the CRS are not compatible.
- 🔌 **Extensible** - Coraza is a library at its core, with many integrations to deploy on-premise Web Application Firewall instances. Audit Loggers, persistence engines, operators, actions, create your own functionalities to extend Coraza as much as you want.
- 🚀 **Performance** - From huge websites to small blogs, Coraza can handle the load with minimal performance impact. Check our Benchmarks
- ⋆ **Simplicity** - Anyone is able to understand and modify the Coraza source code. It is easy to extend Coraza with new functionality.
- 💬 **Community** - Coraza is a community project, contributions are accepted and all ideas will be considered. Find contributor guidance in the CONTRIBUTION document.

WAF



SaaS Security Management

Enterprise grade management and situational visibility using WebUI and management available as SaaS.

ML-Based Threat Prevention (WAF)

Prevents OWASP-10 and zero day threats automatically using ML engine and scoring based on transaction, user behavior, crowd behavior & content risk. No signatures.

API Discovery and Security

Know your API usage and narrow your attack surface to keep API activity within safe limits through ML-based malicious content blocking and OpenAPI schema validation.

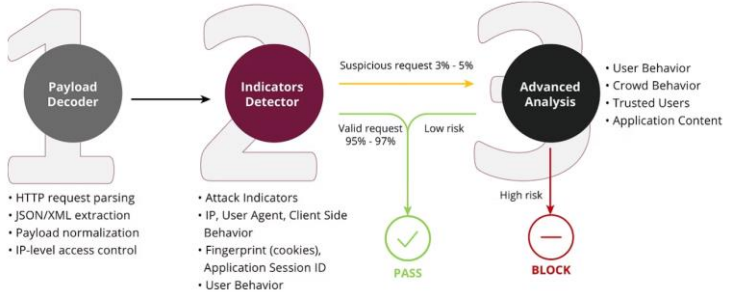
Anti-Bot

Identify and stop automated attacks before intrusion, theft or harm to customer experiences.

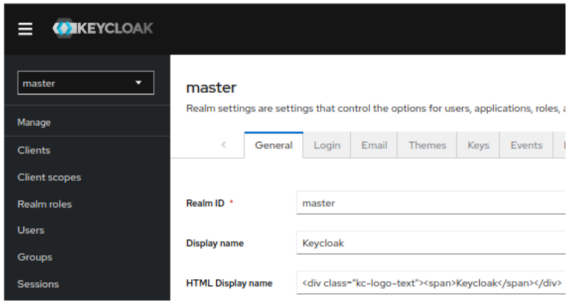
Intrusion Prevention (IPS)

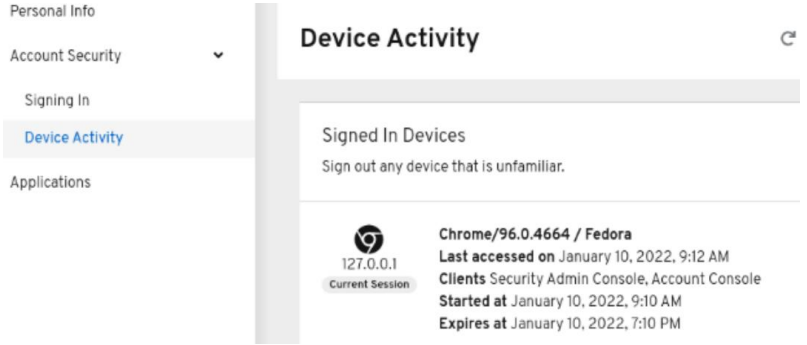
Protect against over 2,800 Web CVEs, based on award winning NSS-Certified IPS and a fully open Snort 3.0.

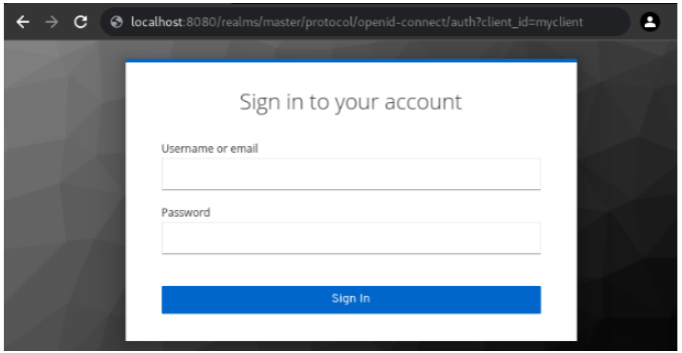
open-appsec
by CHECK POINT

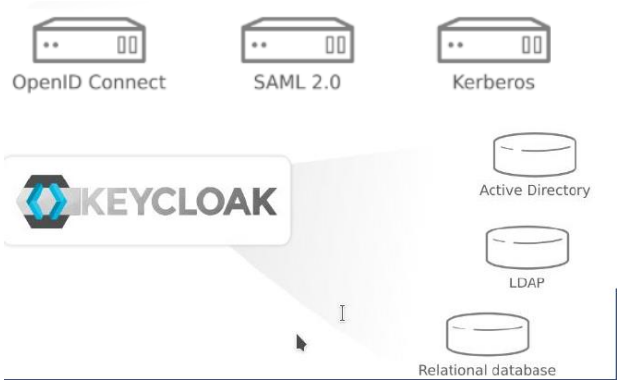


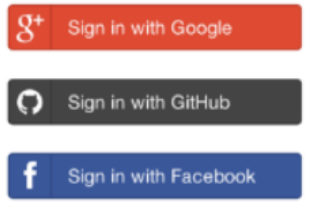
Les identités











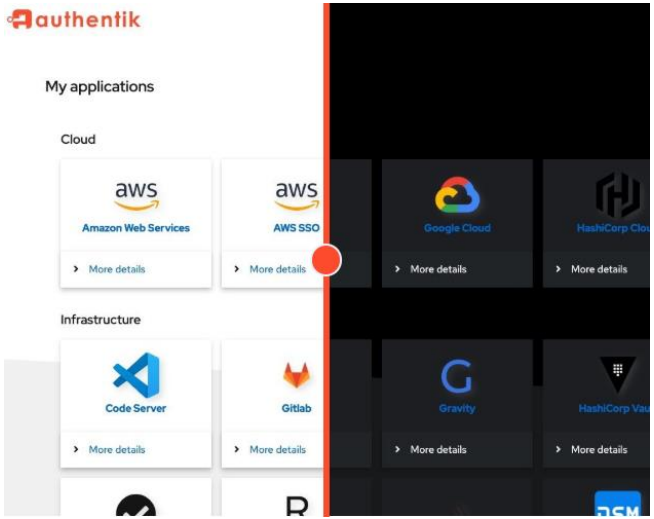
Les identités

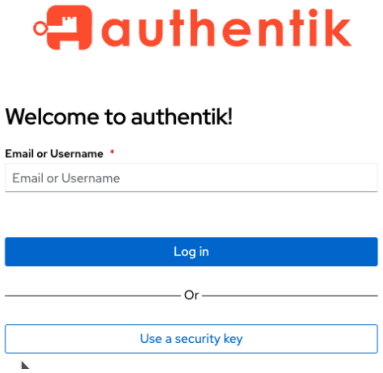
Core Capabilities
Self-host anywhere
MFA ⓘ
Conditional Access
Open-source/Source available
Application Proxy
FIPS Compliance
Enterprise support
WebAuthn (Passkeys)
GeoIP / Impossible Travel
Remote access (RDP, VNC, SSH)

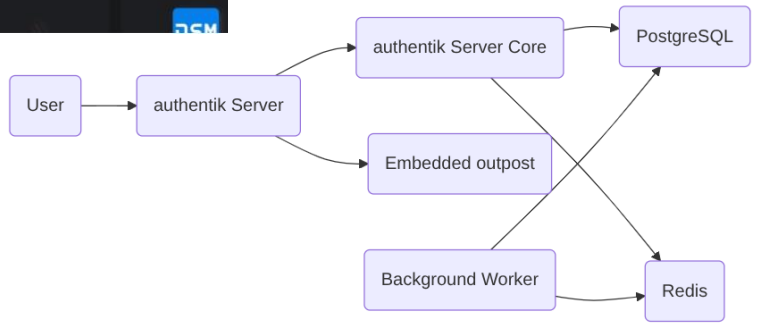
Use cases
Authentication
Enrollment
Self-service

Protocols
OAuth2 / OIDC
SAML2
SCIM
LDAP
RADIUS
SSF (Apple Business Manager)

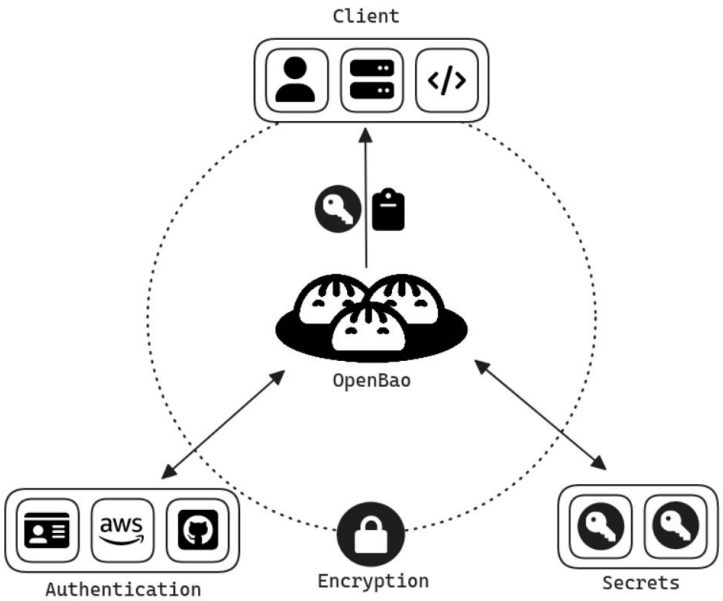
Federation support
OAuth2 / OIDC
OAuth1
SAML2
LDAP
SCIM
Kerberos







KMS



Secure Secret Storage

Arbitrary key/value secrets can be stored in OpenBao. OpenBao encrypts these secrets prior to writing them to persistent storage, so gaining access to the raw storage is not enough to access your secrets.

Dynamic Secrets

OpenBao can generate secrets on-demand for some systems, such as Kubernetes or SQL databases. After creating these dynamic secrets, OpenBao will also automatically revoke them after the lease is up.

Data Encryption

OpenBao provides encryption as a service with centralized key management to simplify encrypting data in transit and stored across clouds and datacenters.

OpenBao

THE LINUX FOUNDATION

Identity based access

Organizations need a way to manage identity sprawl with the use of different clouds, services, and systems. OpenBao solves this challenge by using a unified ACL system to broker access to systems and secrets and merges identities across providers.

Revocation

OpenBao has built-in support for secret revocation. OpenBao can revoke not only single secrets, but a tree of secrets, for example all secrets read by a specific user, or all secrets of a particular type.

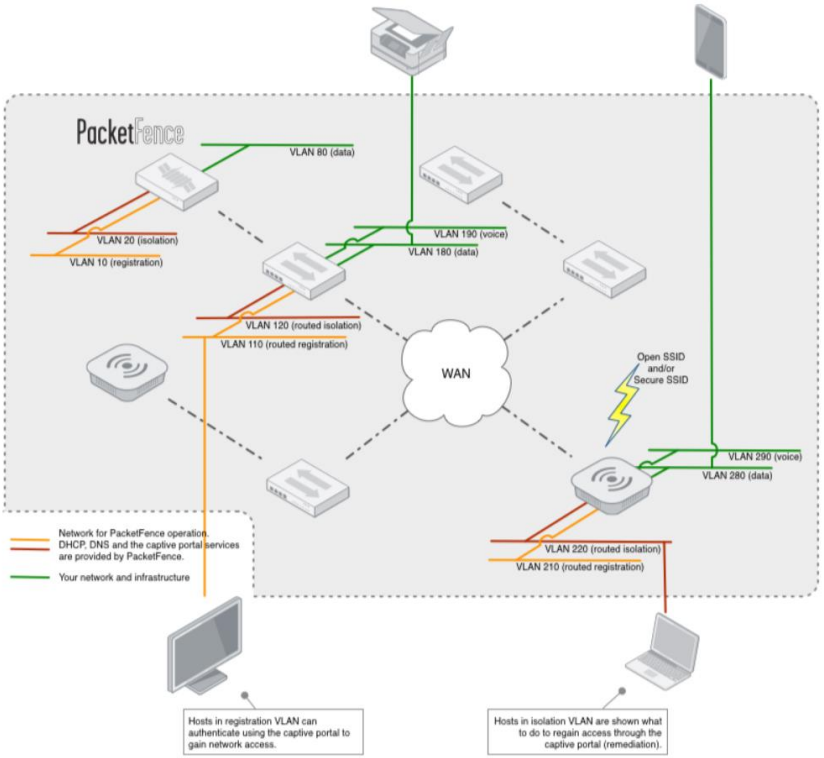
Automatisation de la conformité

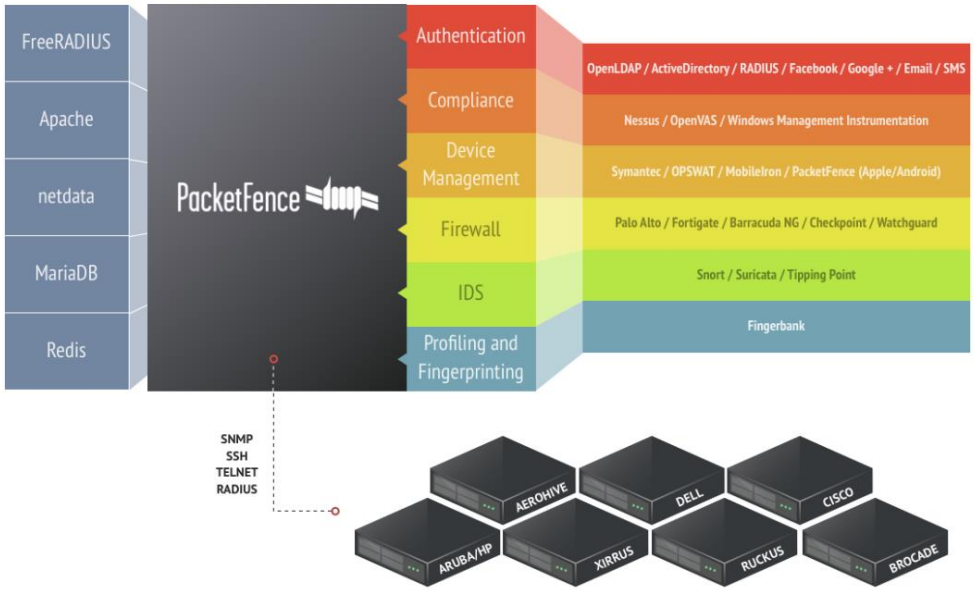
Chef InSpec *is an open-source testing framework with a human- and machine-readable language for specifying compliance, security and policy requirements. When compliance is expressed as code, you can integrate it into your deployment pipeline and automatically test for adherence to security policies.*

Chef InSpec code can run in multiple platforms. You can execute the same set of tests locally, with remote commands that use SSH or WinRM, or with external mechanisms such as the Docker API.

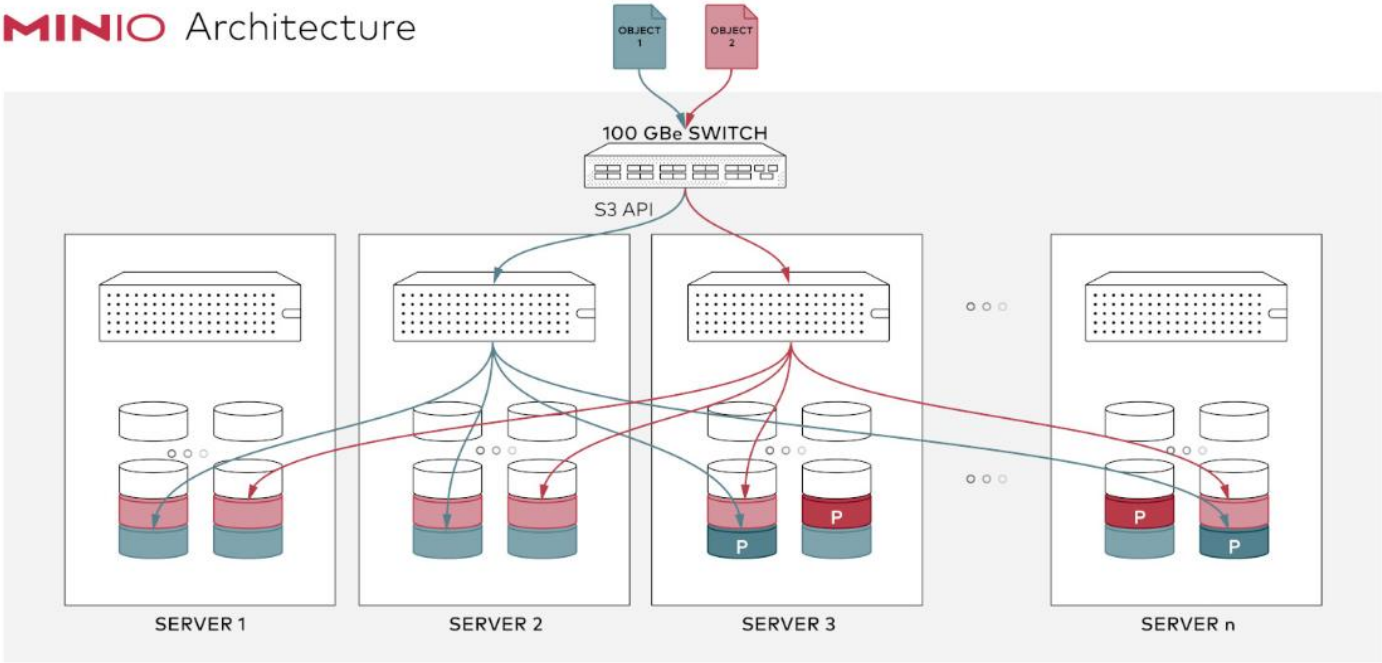

```
describe package('telnetd') do
  it { should_not be_installed }
end

describe inetd_conf do
  its('telnet') { should eq nil }
end
```

Un peu de NAC





L’immuabilité



Présentation RMP V2

Challenges

Les challenges

TELNET - Authentification

NTLM - Authentification

CISCO - Mot de passe

DNS - Transfert de zone

OSPF - Authentification

Netfilter - Erreurs courantes

Web - Serveur : HTTP - Contournement de filtrage IP

BESOIN D'EN SAVOIR PLUS ?

CONTACTEZ-NOUS

ROOT-ME PRO

29 bis chemin de Grave

69450 Saint-Cyr-au-Mont-d'Or

commerce@pro.root-me.org

https://pro.root-me.org