Jacopo Taccucci

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Configurazioni Sicure per Cloud basati su Openstack

GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
ROMA

25/11/2020

Tutor: Prof. Gianluca Reali, Università degli studi di Perugia

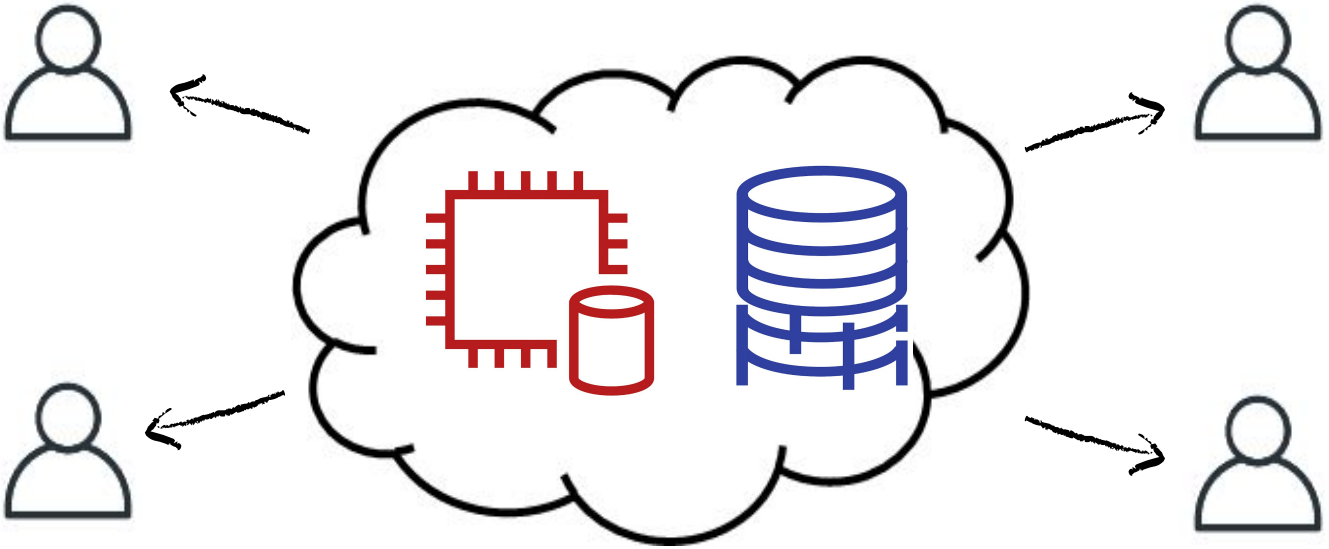
Titolo del Progetto

Definizione e Realizzazione di politiche di auditing per la sicurezza di infrastrutture cloud basate su Openstack

GitHub Repository  git.io/JkXMI

Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

Cloud Computing

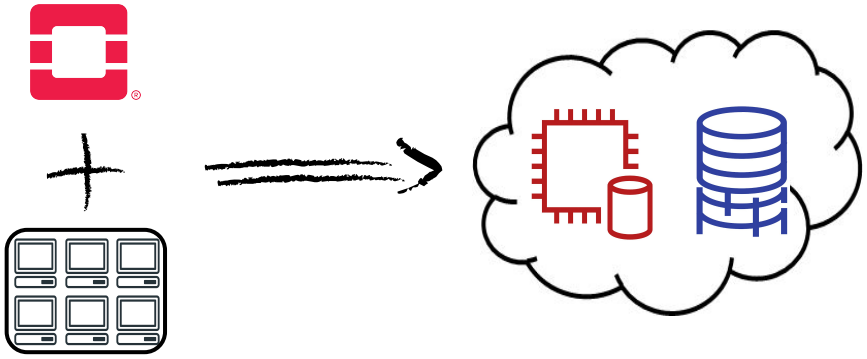


- Self-Service
- Scalabile

Openstack

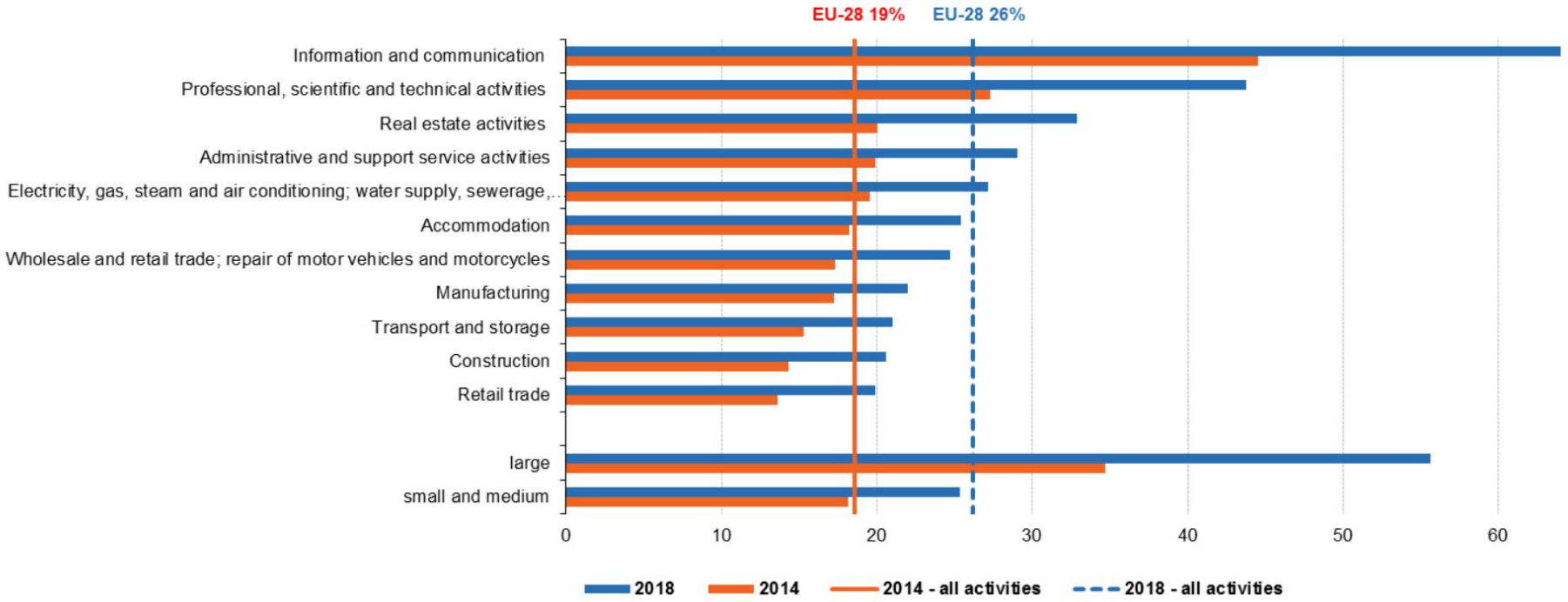
Piattaforma per Cloud Computing

- Opensource
- 9 anni di sviluppo → Maturo
- 63 progetti attivi
- Collaborazione con Rackspace, Suse, Intel ...



Successo Cloud

Utilizzo di servizi di C.C. (% di aziende della zona EU-28):



Fonte: Statistics Explained (https://ec.europa.eu/eurostat/statisticsexplained/) - 24/08/2020

Cloud Computing Security

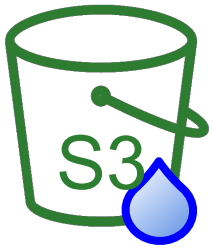
Buckets

Cloud Computing Security

Marzo 2018 → Username e password da un e-shop - **1.3 Milioni** credenziali

Novembre 2017 → Dati sensibili riguardanti votazioni politiche - **198 Milioni** di cittadini coinvolti

Giugno 2017 → Immagine disco di un progetto della NSA - **100GB** di dati riservati



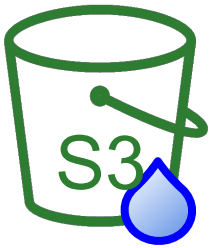
Leaky Buckets

Cloud Computing Security

Marzo 2018 → Username e password da un e-shop - **1.3 Milioni** credenziali

Novembre 2017 → Dati sensibili riguardanti votazioni politiche - **198 Milioni** di cittadini coinvolti

Giugno 2017 → Immagine disco di un progetto della NSA - **100GB** di dati riservati



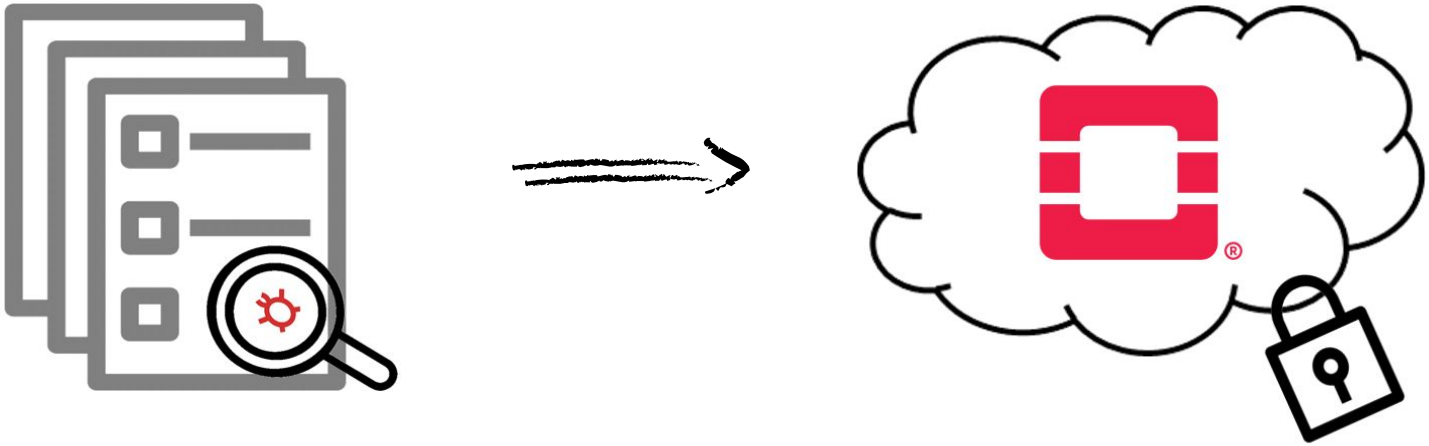
Leaky Buckets

La Causa ?

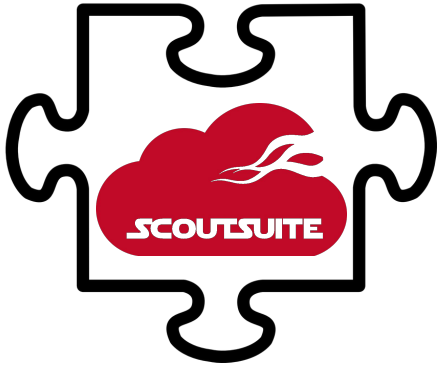
Utente!!!

Obiettivo

Creare uno strumento per identificare configurazioni Vulnerabili.



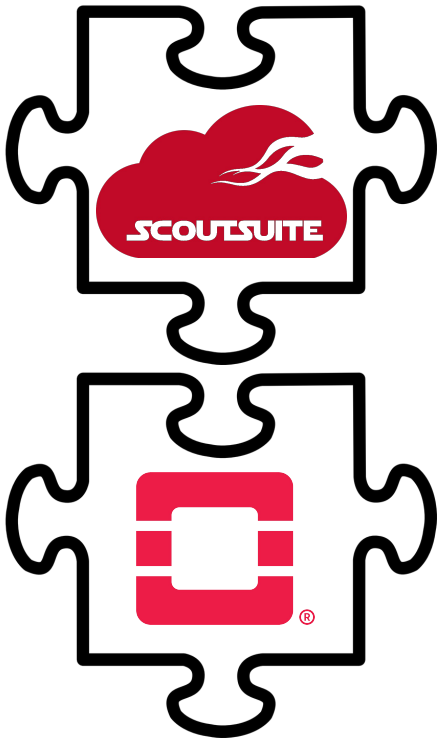
ScoutSuite



Software di Auditing Multi-Cloud

- Opensource
- Nato per AWS
- Modulare
- Basato su Regole da applicare su Risorse

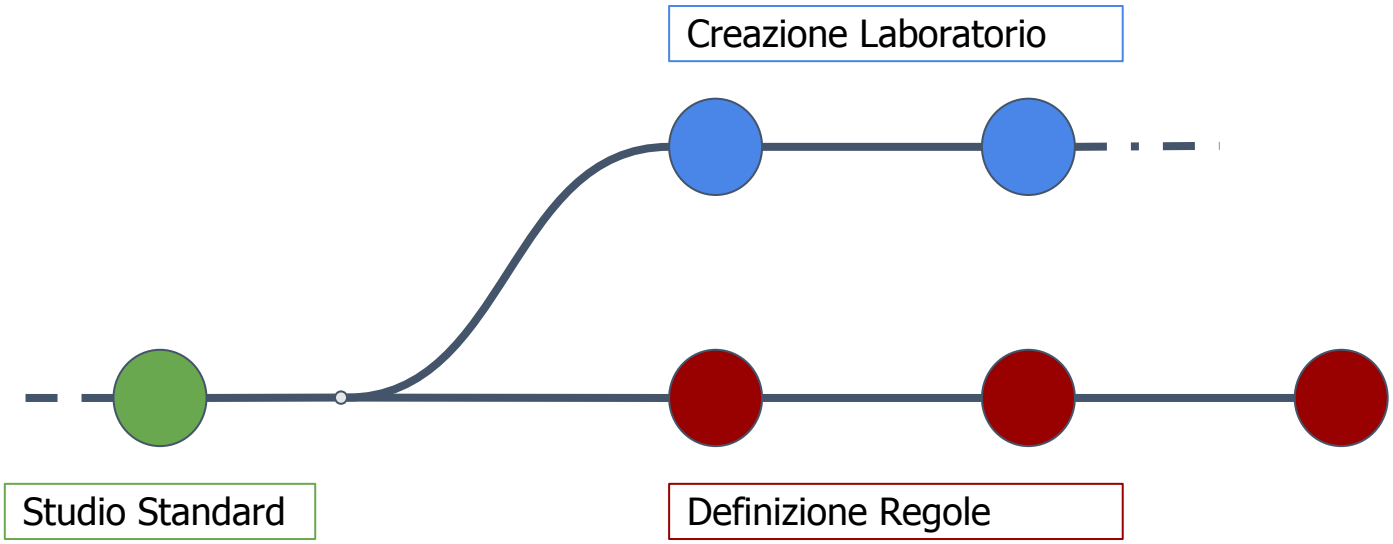
ScoutSuite



Software di Auditing Multi-Cloud

- Opensource
- Nato per AWS
- Modulare
- Basato su Regole da applicare su Risorse

Organizzazione



Documentazione di Riferimento

- **CIS AWS Benchmarks**, *Center for Internet Security*
- **CSA Security Guidance**, *Cloud Security Alliance*
- **Data Security Standard**, *Payment Card Industry Security Standards Council*

- **Cloud Computing: Benefits, risks and recommendations for information security**, *ENISA*

*Fonte Immagine: Film di animazione ***Il mio vicino Totoro*** (となりのトトロ *Tonari no Totoro*), *prodotto da "**Studio Ghibli**"*

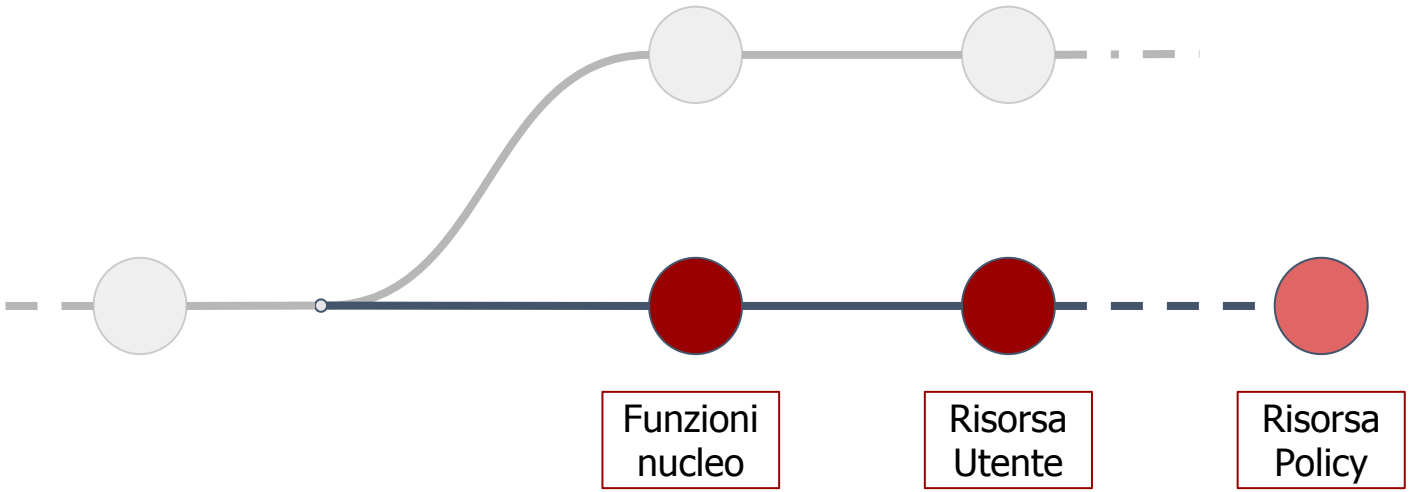
Documentazione di Riferimento

- **CIS AWS Benchmarks**, *Center for Internet Security*
- **CSA Security Guidance**, *Cloud Security Alliance*
- **Data Security Standard**, *Payment Card Industry Security Standards Council*

- **Cloud Computing: Benefits, risks and recommendations for information security**, *ENISA*

*Fonte Immagine: Film di animazione ***Il mio vicino Totoro*** (となりのトトロ *Tonari no Totoro*), *prodotto da "**Studio Ghibli**"*

Definizione Regole



Kill Chain

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Reconnaisance

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

Weaponization & Delivery

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Exploitation

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Installation

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Command & Control & Exfiltration

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Alcune Regole attive nella fase "Exploitation"

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Tipo di Token Utilizzato

Rule : keystone-type-of-used-token

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Nessun Blocco a tentativi di Brute Force

Rule : keystone-lockout-failure-attempts-ignored

PCI - DSS: 8.1.6

Opzione Utente: ignore_lockout_failure_attempts

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

MFA Disabilitato

Rule : keystone-multi-factor-auth-disabled

PCI - DSS: 8.3

CIS AWS Benchmarks: 1.2, 1.13

Opzione Utente: multi_factor_auth_enabled

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Alcune Regole attive nella fase "Installation"

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Condizione di Inattività Ignorata

Rule : keystone-user-inactivity-ignored

PCI - DSS: 8.1.4

CIS AWS Benchmarks: 1.3

Opzione Utente: ignore_user_inactivity

*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Nessuna Scadenza della Password

Rule : keystone-password-expiration-ignored

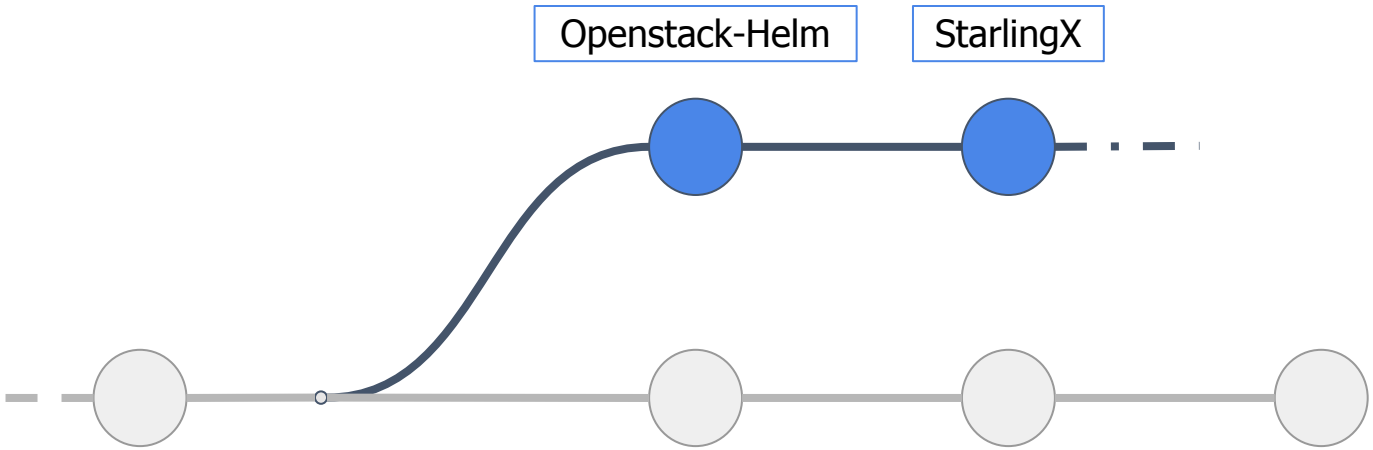
PCI - DSS: 8.2.4

CIS AWS Benchmarks: 1.11

Opzione Utente: ignore_password_expiry

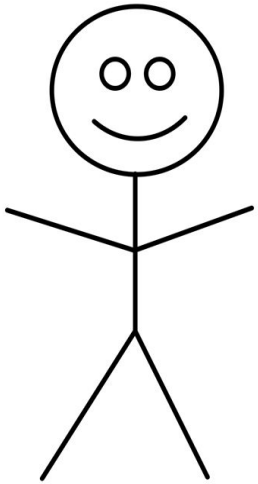
*Fonte Immagine: Netsurion, EventTracker Enterprise and the Cyber Kill Chain
https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

Creazione Laboratorio

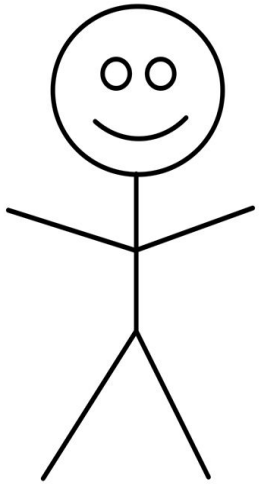


Dream Team

Priscilla Benedetti



Io



Matteo Pergolesi

Lab - Openstack-Helm

Caratteristiche

- Sviluppa un Cloud su Kubernetes
- Basato su Helm - Charts

Problematiche

- Scarsa conoscenza dei Charts Helm
- Progetto poco documentato
- Progetto non ancora in versione stabile

Lab - Openstack-Helm

Caratteristiche

- Sviluppa un Cloud su Kubernetes
- Basato su Helm - Charts

Problematiche

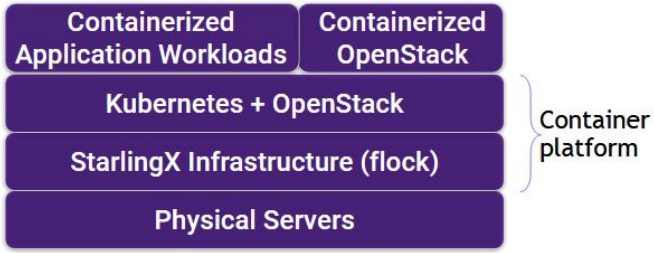
- Scarsa conoscenza dei Charts Helm
- Progetto poco documentato
- Progetto non ancora in versione stabile

Lab - StarlingX

Caratteristiche

- Basato su Openstack e Kubernetes
- Nato per creare Cloud per Edge Computing (bassa latenza)

STARLINGX



- Monta alcuni servizi Openstack su Kubernetes
- Possibilità di usarlo per gli scopi del progetto

Consortium GARR THE ITALIAN EDUCATION & RESEARCH NETWORK

Futuri Sviluppi

Strada Principale

- Analisi della risorsa Policy
- Interpretazione del linguaggio delle Policy tramite un linguaggio standard
- Modellazione delle Policy tramite SAT/SMT

Ispirazione

- "How to shop for free online: security analysis of cashier-as-a-service web stores", Wang et al.
- "SMT Solvers for Software Security", Vanegue et al.

Grazie a tutti!!