OCTARINE

The Kubernetes Common Configuration Scoring System *KCCSS*

February 2020

Introduction

Julien Sobrier

Head of Product, Octarine

- Head of Product at Octarine (K8s Security)
- 10+ years as Security Researcher
- julien@octarinesec.com

Goal for risk framework

- Give a risk score to the workload
- Explain where the risk comes from and what it is
- Show how to remediate the risk

Risk	Name	Kind	Namespace	Domain
9	webserver-for-tests	Deployment	webserver2	cloud:aws-west
8	analysis-kafka	StatefulSet	analysis	cloud:aws-west
5	analytics	StatefulSet	analysis	cloud:aws-west
5	analytics	StatefulSet	development	cloud:aws-west
5	apache	StatefulSet	vm	cloud:aws-west
5	backend	StatefulSet	development	cloud:aws-west
5	baltimore	StatefulSet	inventory	cloud:aws-west

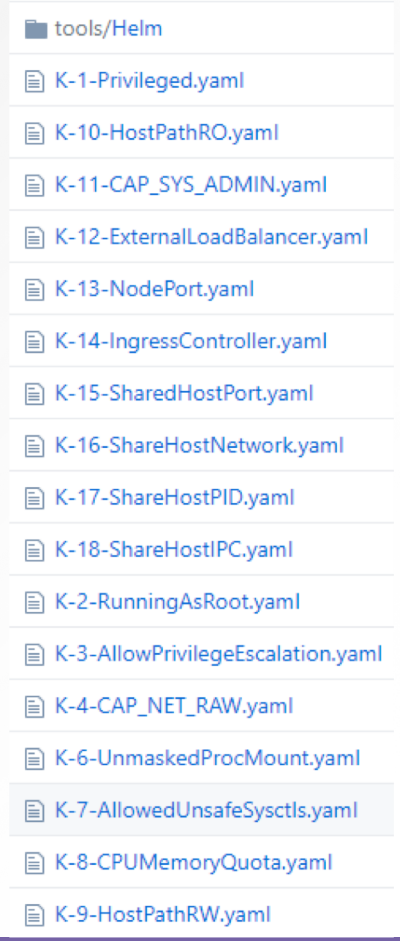
Existing risk frameworks

- CVSS: score vulnerabilities
  - Impact of the risk: Availability, Confidentiality, Integrity
  - Scope of the risk (blast radius)
  - Exploitability, attack vector
- CCSS: CVSS applied to configuration
- CCE: check list of configuration settings

KCCSS

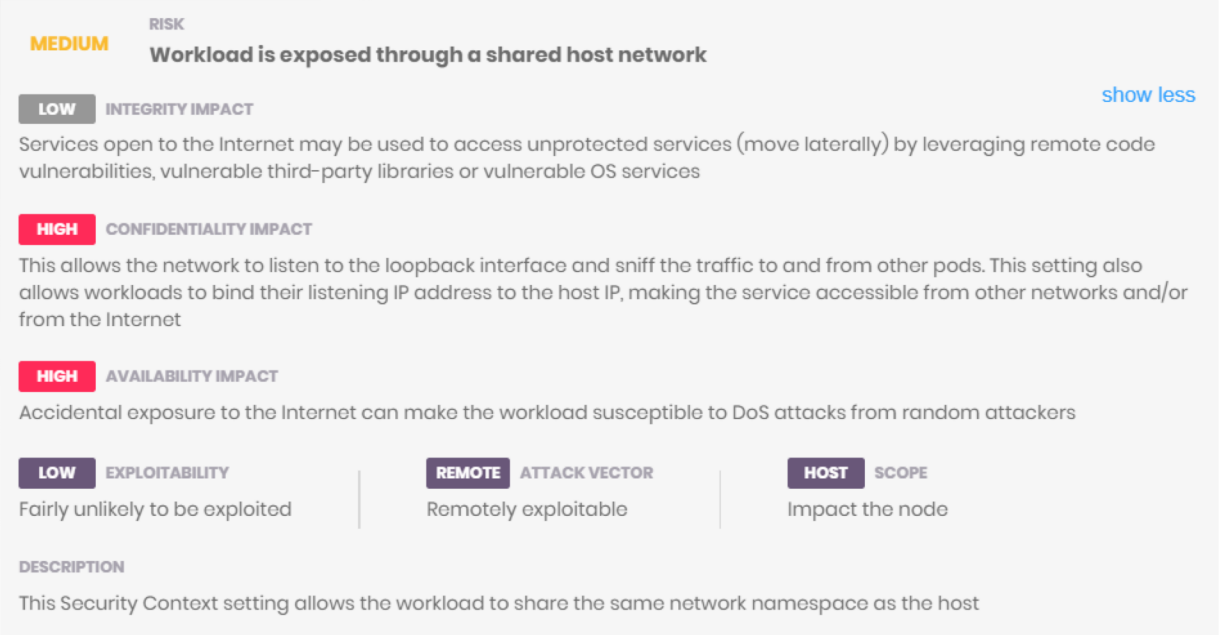
- List of rules (like CCE)
- Same description of rules as CVSS
- Applies to configurations settings (like CCSS)

- NEW: aggregates all risks into a single workload risk
- NEW: specific to Kubernetes



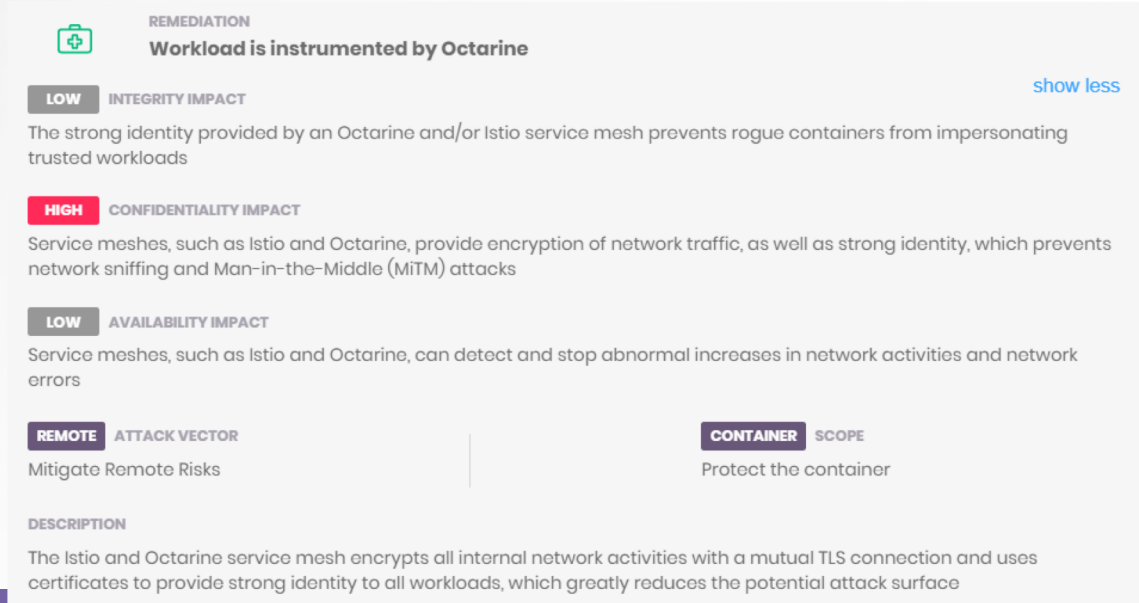
The rules

- Risks
  Impact on Availability, Confidentiality, Integrity
  Exploitability, Attack Vector, Scope
  Description



The rules

- Remediation
  - Lower exiting risk
  - Impact on Availability, Confidentiality, Integrity
    - Attack Vector, Scope



Formulas

1. Rate each risk
   0 (low) to 10 (high)
   Similar to CVSS formula
   Base Impact score = *f*(Availability, Confidentiality, Integrity)
   Impact score = *f*(scope, Base Impact score)

   Exploitability score = *f*(Attack Vector, Exploitability)

   Rule score = Impact score + Exploitability score

Formulas

2. Workload score
   0 (low) to 10 (high)
   Brand new
   Working on improved version

   Scores = Max(Attack Vector ∩ Scope)
   Workload score = $\sqrt{(Score1^2 + Score2^2 + \ldots)}$

Formulas

- Remediations

  For each risk, match remediation with the same attack vector & scope

  Lower corresponding risk impact

  Example:

  Risk: C:H/I:H/A:H

  Remediation: C:L/I:H/A:N

  Final risk: C:M/I:L/A:H

kube-scan

- KCCSS should be used by tools to run the risk score on your workloads
- Kube-scan: open-source workload configuration scanner using KCCSS
    - Install the kube-scan container in your cluster
        - Scan your running workloads
        - See the results though the Web UI

Demo

Further work

- Better matching of remediations and risks
- Improved formula to rate the workload risk
- Additional rules around RBAC
- Additional tools to explore KCCSS

github

- KCCSS: https://github.com/octarinesec/kccss/
- kube-scan: https://github.com/octarinesec/kube-scan

- Learn more: https://www.octarinesec.com/solution-item/kube-scan/

Thank you!

For More Info:

julien@octarinesec.com | www.octarinesec.com

@OctarineSec octarinesec