שם הפרויקט:**Openshift Compliance Framework** (SIEM TOOL)

שמות הסטודנטים: (ת.ז. אימייל וטלפון):

מריאל בורודקין 208584383 [borodkinmariel@gmail.com](mailto:borodkinmariel@gmail.com) 0527244194

ארד גונן 206394579 [aradgonen98@gmail.com](mailto:aradgonen98@gmail.com) 0542256706

התמחות:

סייבר

מאשר הפרויקט:

נצר

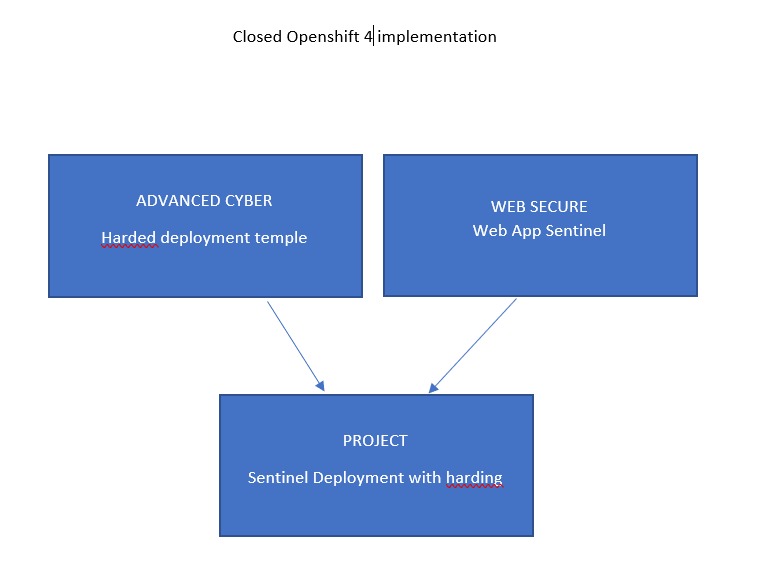
שמות הסטודנטים (אימייל וטלפון):

מריאל בורודקין 208584383 [borodkinmariel@gmail.com](mailto:borodkinmariel@gmail.com) 0527244194

ארד גונן 206394579 [aradgonen98@gmail.com](mailto:aradgonen98@gmail.com) 0542256706

מטרת הפרויקט:

Tool for the compliance framework. The tool is used to deploy compliance policies onto OpenShift clusters and monitor the policies results.

According to our guides, this is the overall solution parted to courses:

מה קיים היום:

כיום יש כלים כלליים שמציגים לוגים ויזואלית אבל אין ממש כלי מיועד עם יכולות רחבות –

* **Collect data at scale and detect** based on Openshift logs for **security information event management** (SIEM) solution.
* **Investigate and respond to incidents rapidly**– Provide **security orchestration automated response** (SOAR) solution of specified tasks.

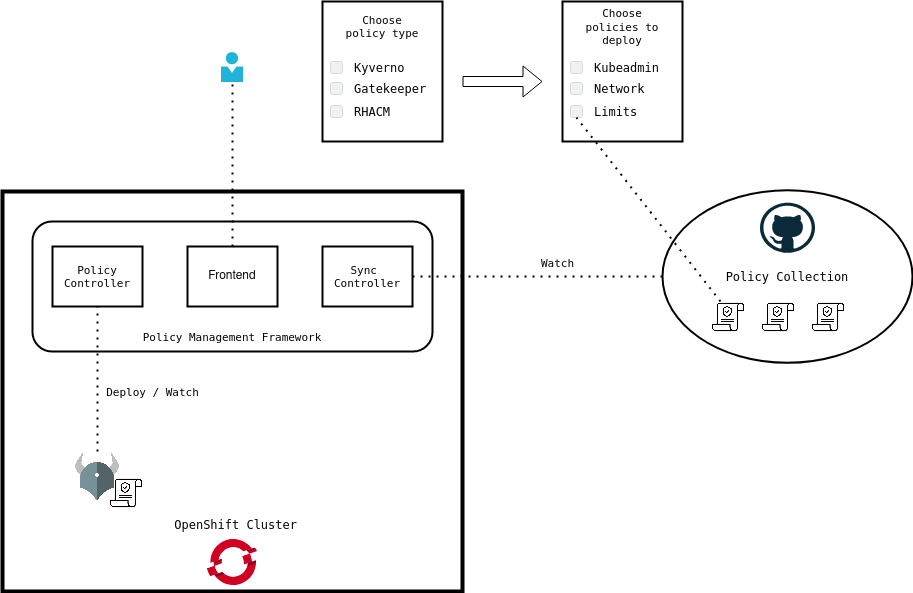
תיאור הפרויקט:

The tool is used by compliance officers in organizations to enforce and visualize compliance status on OpenShift clusters.

אם משתמשים באלגוריתמי למידה או המלצה יש לציין מאיפה תביאו את הנתונים כדי לאמן ולבדוק את המערכת,

תיאור פונקציונאלי בסיסי – מה המערכת תעשה ואיך היא תעבוד

This section describes the deployment of policies to OpenShift environments -



* **Sync Controller** - Used to sync policies from a git repository with the UI. A user can choose to deploy policies from the specified Git repository (as described in the diagram).
* **Frontend** - Allows the user to deploy policies via a wizard that syncs with the sync controller for policy deployment.
* **Policy Controller** - Used to receive data from the user & frontend, and deploy the policies via the specified tool
  + Red Hat Advanced Cluster Management for Kubernetes
  + Open Policy Agent Gatekeeper

טכנולוגיות וסביבת עבודה:

פיתוח אתר WEB בעבור סביבת Openshift 4

**מסמך זה צריך להיות באורך של 3 עמודים.**