ÉCOLE DE L'AIR & DE L'ESPACE
SALON-DE-PROVENCE

SCIICAD - Système Complexe Industriel Interconnecté à un Cyber range d'Attaque et de Défense

DELAGNEAU Etienne

Instructeur et chef de projet
Centre d'Excellence Cyberdéfense aérospatiale
École de l'air et de l'espace

March 20, 2026

Qui sommes-nous ?

Missions :

- Formation : élèves officiers de l'EAE, MS®CyberSCID, formations exportables.
- Innovation : Auprès de l'académique, de la recherche et des industriels.
- PrépaOps : soutien des acteurs opérationnels.

whoami

Etienne Delagneau

- Instructeur et chef de projet du Centre d'Excellence Cyberdéfense aérospatiale
- Président Hack in Provence

etienne.delagneau@ecole-air.fr

SCIICAD

Comment construire un environnement IT/OT réaliste, avec des scénarios reproductibles et un déploiement automatisé, pour expérimenter la détection cyber.

Quelques définitions

- **IT** : Information Technology.
- **OT** : Operational Technology.
- **SIEM** : Security Information and Event Management.
- **SCADA** : Supervisory Control And Data Acquisition.

Besoins

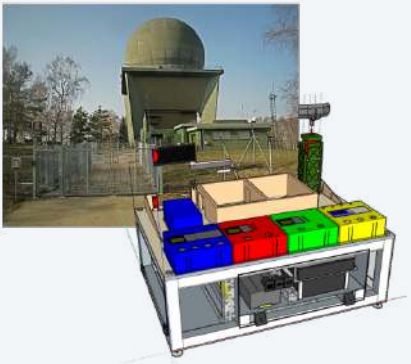
- Générer un **environnement IT et OT réaliste**.
- **Simuler l'activité** d'utilisateurs et de systèmes.
- Intégrer des vulnérabilités et **scénarios d'attaque**.
- Produire des **journaux d'évènement caractéristiques**.
- Permettre la **supervision et la détection**.
- Assurer la **reproductibilité** des scénarios.

Cahier des charges

- **Environnement académique / pédagogique**.
- **Déploiement automatisé**.
- **Flexibilité et modularité**.
- **Solutions libres et reproductibles**.
- **Observabilité**.

Projet SCIICAD

Système **Complexe** Industriel Interconnecté à un Cyber range d'**Attaque** et de **Défense**



Vue fonctionnelle

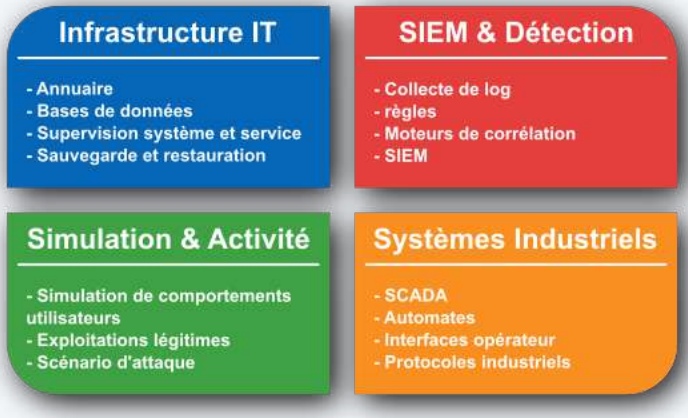
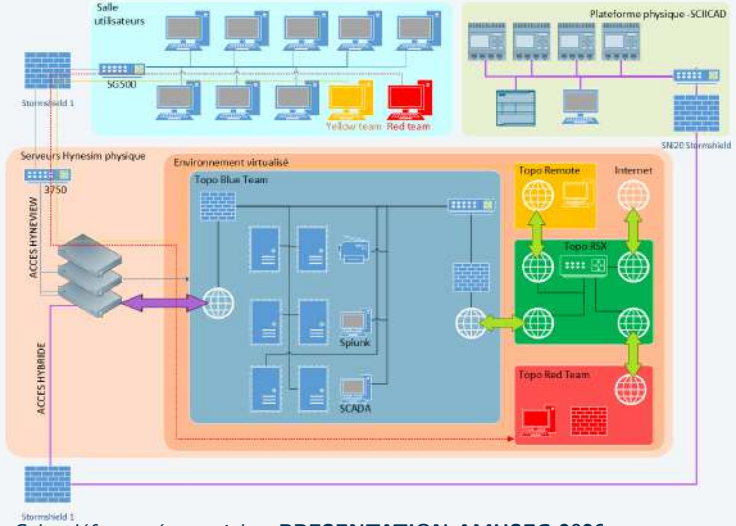


Diagramme d'infrastructure logique



Génération d'activité sur SCIICAD

- **Rappel d'objectif** :
  Génération de traces réalistes.

Génération d'activité sur SCIICAD

- **Rappel d'objectif** :
  Génération de traces réalistes.

- **Activités légitimes**.
  Maintenance, tests, mises à jour. Vidéo : **video_sciicad.mp4**
- **Simulation utilisateur automatisé** :
  Playwright et Selenium.
- **Scénarios automatisés** :
  Sur systèmes et scénarios d'attaque (IT/OT).

Scénario d'attaque

Exemple : Attaques cyber contre les déploiements OPC UA

Vulnérabilité

- Absence de PKI publique en OT
- 38/48 solutions analysées par l'institution CISPA présentent des erreurs liées aux listes de confiance

Exploitation

- Attaque PitM
- Rogue client
- Rogue server

Cycle de vie des logs et alertes

Sources de logs IT/OT
workstations, serveurs, PLC, SCADA, IHM, équipements et sondes réseau

↓

Collecte des logs IT/OT
Filebeat, Winlogbeat, auditd, OPC-UA Logger, Syslog, NetFlow

↓

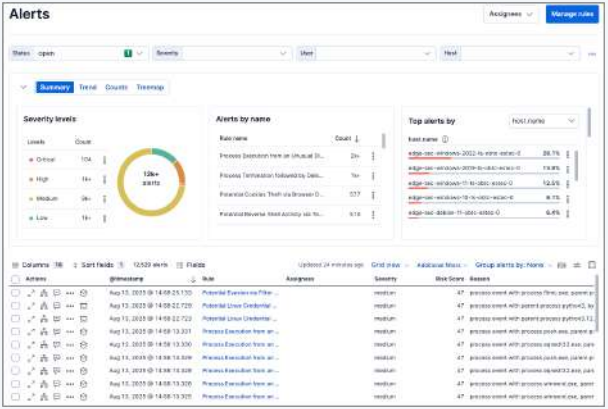
Ingestion et normalisation
ELK, Splunk, Wazuh

↓

Règles de détection
SIGMA, Wazuh rules, Splunk SPL, YARA

↓

Alertes / Tickets
Wazuh + TheHive



Simulation OT

- Développement interne d'un **GDS open-source** en python.
- Gestion automatisée des certificats et de la sécurité.
- Création d'environnements OT modulaires et flexibles.
- **Respect des standards OPC UA** : chiffrement et authentification.
- Simulations reproductibles, scalables et partageables.

Infrastructure as Code (IaC)

Infrastructure as Code : approche permettant de gérer et déployer une infrastructure informatique **à l'aide de code** plutôt que par des actions manuelles.

- **Terraform** : provisionnement de l'infrastructure (VM, réseaux, hyperviseur).
- **Packer** : création automatisée d'images systèmes reproductibles (templates de VM).
- **Ansible** : configuration et déploiement des logiciels sur les machines.

Pipeline IaC typique

$$\text{Packer} \rightarrow \text{Terraform} \rightarrow \text{Ansible}$$

Comparatif Cyber Range vs Déploiement IaC

	Cyberrange	**Déploiement IaC**
Forces	- Plateforme prête à l'emploi - Support fourni par le fabricant - Monitoring intégré - Rejeu facile	- Flexibilité - Reproductible et versionnable via Git - Automatisation des déploiements - Open source
Faiblesses	- Infrastructure support rigide - Dépendance au fabricant - Coût élevé des licences	- Courbe d'apprentissage importante - Documentation à créer et maintenir - Supervision à charge de l'équipe - Destruction accidentelle possible - Temps de mise en service supérieur

Infrastructure Support

Site télégérant

- Serveurs : 2 x Lenovo x3650 M4
- Stockage : 2 x Dell ME512

Site distant

- Serveur automate : S7-1200
- Microcontrôleur PLC : 4 x Siemens LOGO8
- Serveur HMI + Historian : Lenovo ThinkCentre i5
- Pare-feu : Stormshield SN210

Capacité et utilisation de l'infrastructure

Usage

- Capacité : 288 vCPU, 1.5 To RAM
- Emploi : 33 vCPU, 273 GiB RAM, 47 entités

Visualisation

Supervision infrastructure support

- **Supervision infrastructure** : monitoring des VM hébergées sur Proxmox.
- **Observabilité système** : collecte de métriques et journaux.
- **Bastion d'accès** : Teleport pour l'accès sécurisé aux ressources.
- **Traçabilité** : journalisation des actions utilisateurs et administrateurs.

Feuille de route SCIICAD

- **Phase 1 — Conception** : architecture IT/OT et maquette industrielle
- **Phase 2 — Prototype** : cyber range Hynesim, premiers scénarios
- **Phase 3 — Plateforme expérimentale** : supervision, SIEM, génération d'activité
- **Phase 4 — Industrialisation** : migration Proxmox HA et IaC
- **Phase 5 — Recherche avancée** : simulation OT, GDS open-source, partage scientifique

Conclusion

- **Plateforme IT/OT réaliste**.
- **Respect des standards d'authentification et de sécurisation d'OPC Fondation**.
- **Génération de données** d'activité et de journaux exploitable.
- Scénarios **reproductibles** via IaC.
- Collaboration et **partage** pour l'innovation industrielle.

```
# packer_build.sh
echo "[Packer] Initializing VM image..."
sleep 2
echo "[Packer] Installing base OS... done"
sleep 1

echo

[Packer] Image ready for
Terraform deployment!
```

```
# terraform_apply.sh
echo "[Terraform] Planning infrastructure..."
sleep 2
echo "[Terraform] Provisioning servers... done"
sleep 1

echo

[Terraform] Ready to configure
with Ansible!
```

```
# ansible_playbook.sh
echo "[Ansible] Applying playbooks..."
sleep 2
echo "[Ansible] Apps configured and running"
sleep 1

echo

[Ansible] Conference done!
Au plaisir d'échanger autour d'un verre !
```

Contact

Projet SCIICAD

Centre d'excellence cyberdéfense aérospatiale
Direction Générale de l'enseignement et de la Recherche /
Ecole de l'air et de l'espace

Email : etienne.delagneau@ecole-air.fr

Merci pour votre attention

Cyb'Air Sud

Thème :
Les vulnérabilités matérielles et la sécurité industrielle

Dates :
Mardi 24 novembre 2026

Lieu :
Base aérienne 701
Ecole de l'air et de l'espace
Salon de Provence

ÉCOLE DE L'AIR
& DE L'ESPACE
SALON-DE-PROVENCE

CENTRE D'EXCELLENCE
CYBERDEFENSE
AEROSPATIALE

SCIICAD - AMUSEC 2026

DELAGNEAU Etienne

Instructeur et chef de projet
Centre d'Excellence Cyberdéfense aérospatiale
École de l'air et de l'espace

March 20, 2026