Anàlisi de riscos d'una empresa

Neuchâtel-Energie

Alumne: Hamza El Haddad Sabri , Nicolau Mesalles Campos i Oscar Saborido Valdes

Data: 03/12/24 - 06/01/25

Índex

Introducció

Solament és necessària una cerca ràpida a internet per trobar estadístiques que demostrin que la ciberdelinqüència està més activa que mai. Tot i que les grans empreses fan tot el que poden per evitar ser afectades per aquest fenomen, és virtualment impossible ser 100% invulnerable a atacs. Una de les indústries on un atac cibernètic pot significar un perill crític és la nuclear, com ha quedat demostrat amb incidents reals com el cas de Stuxnet, que va afectar les instal·lacions nuclears de l'Iran. Un atac podria produir el robatori de materials radioactius residuals, el mal funcionament d'un reactor o l'alliberament de radiació a l'atmosfera, amb un impacte catastròfic tant per al medi ambient com per a la salut humana. Finalment, també afecta la imatge, ja criticada, que té aquesta energia de baixes emissions. En aquest anàlisi es tractaran els diferents riscos cibernètics als quals s'enfronta una central nuclear i com evitar-los. Es faran recomanacions de ciberseguretat i com aquestes afecten l'empresa de manera econòmica, social i jurídica. Tanmateix, es farà la simulació d'un atac, recreant un escenari plausible com un atac ransomware o una intrusió a la xarxa SCADA, i s'analitzarà com contrarestar-lo amb mesures reactives i preventives.

Context de l'empresa

L'empresa fictícia que hem creat està estretament relacionada amb aquest àmbit, ja que és una empresa dedicada a la construcció, manteniment de plantes nuclears, així com la seva posada en marxa i utilització. Amb aquest treball esperem plasmar la importància que té mantenir els sistemes d'una central nuclear protegits enfront de possibles amenaces i com la intrusió i alteració del funcionament normal d'una central nuclear pot ocasionar una catàstrofe.

Neuchâtel-Énergie és una empresa que pertany al sector de l'energia nuclear. Té centrals a tot el món, incloent-hi: Montreal, Suïssa, Estats Units, Espanya, França, Regne Unit, Mèxic, Japó, Austràlia, entre d'altres. Compta amb més de 200.000 empleats i té uns ingressos anuals d'uns mil milions d'euros. Tot i ser reconeguda a

escala mundial per les seves plantes nuclears, també es dedica a la investigació sobre l'energia nuclear, mineria d'urani i subministrament d'aquest mateix, així com el tractament i enriquiment de l'urani per ser utilitzat a les seves plantes.

La infraestructura de l'empresa es compon d'una xarxa tecnològicament avançada que fusiona serveis al núvol i locals per garantir la seguretat i el correcte funcionament dels seus actius més crítics:

- **Reactors nuclears:** Aquests són el cor de la planta nuclear. Sempre en constant monitoratge per sistemes automatitzats. Diferenciem entre reactors d'aigua pressuritzada i d'evaporació d'aigua. Els dos fan la mateixa funció, però de maneres diferents.
- **Serveis al núvol:** L'empresa utilitza serveis com AWS i Azure per al processament i emmagatzematge de la informació de manera centralitzada i garantint-ne la seguretat.
- **Xarxes SCADA i IoT:** L'empresa utilitza sensors IoT en temps real per monitorar la temperatura, pressió, nivells de radiació i fluxos de refrigerant en els reactors, i assegurar que funcionen de manera correcta.
- **Sistemes de telecomunicacions:** Una xarxa global interconnectada per assegurar que els serveis de cap central no es vegin interromputs de cap manera.
- **Bases de dades:** L'empresa emmagatzema dades sobre el manteniment, historial del funcionament, protocols de seguretat i dades científiques de recerca. Sistemes com aquests es poden veure afectats per atacs de ransomware o per atacs que busquin una fallada crítica del sistema per ocasionar malfuncionaments.

Objectius

L'objectiu principal d'aquest exercici és dur a terme una anàlisi exhaustiva de riscos sobre Neuchâtel-Énergie per identificar, analitzar i mitigar les amenaces potencials que una empresa d'energia nuclear pot sofrir. El treball s'enfocarà a oferir solucions específiques per als sistemes crítics de l'empresa.

Metodologia

Tota la investigació realitzada per aquest document ha estat feta a partir de fonts fidedignes i oficials, tals com CISA, EUR-Lex, Servei de Seguretat Federal, Ciberseguridad.com, NIST, MITRE ATT&CK. També s'han analitzat informes forenses de ciberseguretat sobre incidents reals en plantes nuclears. Les normatives més extenses i normalitzades són les europees i nord-americanes, però cal considerar que altres països tenen lleis diverses que poden diferir d'aquests marcs. S'han implementat frameworks com el de NIST, reconegut per la seva efectivitat en la gestió de riscos cibernètics, per estructurar i guiar aquest treball. També es faran mencions a certes aplicacions que se sobreentén que el lector ja coneix; en cas contrari, consulteu la webgrafia.

El treball està diferenciat en tres etapes principals: identificació d'actius crítics, anàlisi de possibles riscos i, finalment, proposta de les mitigacions pertinents.

Possibles disparitats

La informació proporcionada en aquest document podria haver estat influenciada per la gran quantitat de dades disponibles i per la manca d'experiència dels redactors en algunes matèries. Tot i que hem intentat ser el més professional possible, és probable que alguna part del contingut pugui contenir errors. En cas de detectar-ne, agraïm que qualsevol correcció ens sigui adreçada a oscar.saborido@enti.cat, hamza.elhaddad@enti.cat o nicolau.mesalles@enti.cat. Us agraïm la vostra comprensió i disculpeu les possibles molèsties.

Identificació i classificació d'actius

Per garantir una anàlisi completa la identificació i classificació dels actius ha estat separada en actius físics i actius lògics. En un context nuclear la correcta protecció i preservació d'aquests actius és fonamental, ja que les conseqüències del seu mal funcionament són catastròfiques.

Els actius s'han classificat en:

- **Actius físics**: Dispositius, maquinària i equips físics de les plantes nuclears. (IIoT)
- **Actius lògics**: Sistemes de programari, bases de dades, xarxes i aplicacions al núvol. (Azure)

Actius físics

Tipus d'Actiu	Fabricant/Model	Funció	Ubicació
1. Sensors IoT (Temperatura)	Siemens/SIMATIC IOT2040	Monitoratge de temperatura als reactors en temps real. Un sobrecalfament del reactor pot portar a l'explosió d'aquest mateix. És obligatori el seu ús.	Es troba a tots els reactors 1-20
2. Sensors IoT (Radiació)	Honeywell/RadEye SPRD	Control en temps real dels nivells de radiació. Com més radiació allibera un reactor	Zones de contenció, zones on la radiació pugui arribar.

		més energia produeix. El seu us és obligatori.	
3. PLCs (Control)	Schneider/Modicon M580	Control dels processos automatitzats	SCADA/Plantes nuclears
4. Dispositius SCADA	ABB/Ability System 800xA	Monitoratge i control dels processos de la planta nuclear.	Sales de control de les plantes.
5. Servidors físics	Dell/PowerEdge R740	Emmagatzematge i processament local de dades al servidor físic.	Centres de dades de la planta (és a nivell local)
6. Switches de xarxa	Cisco/Catalyst 9300	Interconnexió de dispositius de xarxa	Infraestructura IT
7. Càmeres de seguretat	Bosch/DINION 5100i IR	Vigilància física de les plantes.	Zones sensibles
8. Sensors IoT (Pressió)	Yokogawa/EJA 530E	Mesuren pressió en líquids, gasos o vapor amb alta precisió. Suporten protocols	Es troben als reactors nuclears.

		avançats (HART, Fieldbus, PROFIBUS). Són ràpids, i aptes per entorns industrials exigents amb atmosferes perilloses o explosions potencials. amb certificació de seguretat SIL 2.	
9. Dispositius endpoints	HP /ProBook 650 G8	Estacions de treball del personal tècnic. Ja que tots treballen amb el mateix dispositiu, les mesures de seguretat es podran polir i perfeccionar més. (Portàtils)	Oficines tècniques i de treball.
10. Control d'accés físic	HID® iCLASS® SE™ R40	És un lector de paret, compatible amb targetes, clauers i telèfons mòbils. Ofereix seguretat avançada amb el model Secure Identity Object™ (SIO™), que afegeix encriptació extra per protegir dades d'identificació, i utilitza l'Open Supervised Device Protocol (OSDP) per garantir comunicacions	Totes les portes de la central.

Actius lògics

Tipus d'Actiu	Tecnologia	Funció	Ubicació
1. Servidors al núvol (AWS)	Amazon EC2, S3	Emmagatzematge de dades operatives i seguretat.	AWS Cloud
2. Servidors al núvol (Azure)	Microsoft Azure VMs	Emmagatzematge per anàlisi de dades crítiques.	Azure Cloud

3. Bases de dades crítiques	Oracle Database 19c	Informació de manteniment i seguretat nuclear.	Centres de dades
4. Sistemes SCADA	ABB Ability System 800xA	Control remot i supervisió d'actius físics.	Xarxa interna
5. Xarxa de telecomunicacions	Cisco SD-WAN	Interconnexió de xarxes a escala global.	Infraestructura IT
6. Firewall i IDS/IPS	Palo Alto PA-5250	Protecció perimetral de la xarxa. Aquest Firewall es el rpimer del món amb aprenentatge automatic. El que interessa principalment es la seva ZeroTrust amb dispositius IoT.	Infraestructura IT
7. Aplicacions IoT	Siemens MindSphere	Gestió i visualització de dades dels sensors. És el sistema operatiu amb el que els dispositius IoT operen.	Núvol i SCADA

8.Sistemes Enterprise Resource Planning (ERP)	SAP S/4HANA	Gestió empresarial (logística i finances)	Oficines principals
9. Eines de ciberseguretat	Splunk Enterprise	Monitorització d'incidents i logs. L'aplicatiu d'questa empresa permet l'analisi del sistema, prevenciio de riscos i resposta enfront d'incidents de manera rapida i efectiva.	Infraestructura IT
10. Sistemes de backup	Veeam Backup & Replication	Còpia de seguretat de dades crítiques. És l'empresa 1º a nivell mundial dedicada exclusivament a la conservació de dades i la recuperació de les mateixes.	Centres de dades

Classificació dels actius segons importància i impacte potencial

Per classificar els actius segons la seva **importància** i l'**impacte potencial**, s'han utilitzat tres criteris principals:

- **Impacte sobre la seguretat**: Quin és el risc per a la seguretat física i mediambiental si un actiu falla o és atacat.
- **Impacte sobre les operacions**: Quina afectació tindria la interrupció de l'actiu en el funcionament normal de la planta nuclear.
- **Impacte econòmic**: Quin seria el cost econòmic associat a una fallada o compromís de l'actiu.

Tenint en compte aquest criteri els actius han estat separats en quatre categories:

- **Nivell Alt:** Fallada catastròfica per a la central, el medi ambient i l'empresa. Actius crítics.
- **Nivell Mitjà-Alt:** Fallada significativa amb impacte important, però no tan crítica com al nivell alt.
- **Nivell Mitjà:** Fallada que provoca tancament temporal de la central sense afectar l'empresa globalment.
- **Nivell Baix:** Fallada amb impacte limitat i malfuncionament parcial sense tancament.

Nivell Alt

Tipus d'Actiu	Tecnologia
Sensors IoT crítics	Sensors de radiació (Honeywell/RadEye SPRD), Sensors de temperatura (Siemens/SIMATIC IOT2040), Sensors de pressió (Yokogawa/EJA530E)
Dispositius SCADA	ABB/Ability System 800xA

PLCs	Schneider/Modicon M580
Control d'accés físic	HID iCLASS SE R40
Bases de dades crítiques	Oracle Database 19c
Sistemes SCADA	ABB Ability System 800xA

Nivell Mitjà-Alt

Tipus d'Actiu	**Tecnologia**
Servidors físics	Dell/PowerEdge R740
Xarxa de telecomunicacions	Cisco SD-WAN
Sistemes de backup	Veeam Backup & Replication

Eines de ciberseguretat	Splunk Enterprise

Nivell Mitjà

Tipus d'Actiu	Tecnologia
Servidors al núvol	AWS (Amazon EC2, S3), Azure (Microsoft Azure VMs)
Sistemes ERP	SAP S/4HANA
Aplicacions IoT	Siemens MindSphere
Col·lector de dades IIoT	Encardio Rite/Datalogger for Digital Sensors

Nivell Baix

Tipus d'Actiu	Tecnologia
Dispositius endpoints	HP ProBook 650 G8

Càmeres de seguretat	Bosch/DINION 5100i IR
Switches de xarxa	Cisco Catalyst 9300

Identificació de Riscos

Tot i que l'energia nuclear és una de les fonts energètiques més eficients i sostenibles, té riscos bastant elevats debut a la seva complexitat, a més els impactes solen ser molt greus, és per això que s'ha de tenir molta cura i tenir els riscos ben controlats.
A l'empresa de Neuchâtel-Energie s'han separat els riscos en dos sectors:

- **Amenaces**: atacs cibernètics o sabotatges.
- **Vulnerabilitats**: errors humans, configuracions inadequades o seguretat digital poc robusta.

Amenaces detallades amb descripció tècnica

ID - Tècnica	Amenaces	Descripció Tècnica	Actius Afectats
T1021.002 - Remote Services: SMB/Windows Admin Shares	Accés no autoritzat als sistemes SCADA	Els adversaris poden utilitzar credencials vàlides, és a dir, obtenir i abusar de les credencials de comptes existents, per accedir i operar recursos de xarxa remots mitjançant SMB, actuant com l'usuari legítim.	SCADA, PLCs, IoT, xarxes.
T1486 - Data Encrypted for Impact	Atacs de xifratge a Bases de Dades	Els atacants poden xifrar arxius per bloquejar l'accés als recursos, amb l'objectiu d'extorsionar econòmicament (ransomware) o fer la informació inaccesssible.	Bases de dades, servidors, backups.

T1040 - Network Sniffing	Intercepció de dades	Els atacants poden interceptar el trànsit de xarxa amb interfícies en mode promiscu per obtenir credencials no xifrades o informació sensible.	IoT, SCADA, xarxes.
T1499 - Endpoint Denial of Service	Atacs DDoS	Els atacants poden llançar atacs de denegació de servei (DoS) o DDoS(DoS generat per diversos sistemes distribuïts per Internet) per degradar o bloquejar la disponibilitat dels serveis als usuaris.	Xarxes, núvol, SCADA.
T1210 - Exploitation of Remote Services	Explotació de Controladors d'Accés Remot	Els atacants podrien aprofitar vulnerabilitats en controladors d'accés remot o RDP mal configurats per obtenir accés inicial als sistemes crítics.	Xarxes internes, sistemes SCADA, servidors locals.
T1071 - Application Layer Protocol	Comunicacions amb C2 Mitjançant Proxies	Els atacants podrien utilitzar proxies per camuflar la comunicació amb servidors de comandament i control (C2), evitant ser detectats.	Xarxes de telecomunicacions, servidors al núvol.

T1074 - Data Staged	Robatori de Dades Crítiques	L'exfiltració de dades sensibles podria ser realitzada aprofitant eines d'encriptació per ofuscar les transferències de dades fora de la xarxa.	Bases de dades, sistemes de backup.
T1203 - Exploitation for Client Execution	Explotació de vulnerabilitats als aplicatius per executar codi.	Explota vulnerabilitats en aplicacions del client, com navegadors o editors de documents, per executar codi maliciós al sistema objectiu, permetent comprometre'l i desplegar malware o escalar privilegis	IoT, Xarxa, Servidors al núvol, Sistemes backup, Base de dades
T1055 - Process Injection	Injecció de codig i possible escalabilitat de privilegis.	Implica injectar codi maliciós en processos legítims del sistema per executar-lo amb els permisos del procés objectiu, millorant l'evasió de detecció i permetent accions com accés a memòria, persistència o escalat de privilegis.	Servidors locals, Base de dades, PLCs, Sistemes backup
T1566.002 - Phishing: Spearphishing Link	Robatori de credencials	Utilitza correus electrònics personalitzats amb enllaços maliciosos per enganyar la víctima i aconseguir que accedeixi a llocs web que roben credencials o executen codi maliciós, permetent comprometre sistemes o obtenir informació sensible.	IoT, Xarxa, SCADA, Servidors al núvol, Sistemes backup, Base de dades, Servidors locals, PLCs

Anàlisi de vulnerabilitats

	ID - Tècnica	Vulnerabilitats	Descripció Tècnica	Actius Afectats
Vulnerabilitats Internes	T1078 - Valid Accounts	Configuracions inadequades en dispositius IoT	Ús de credencials robades mitjançant configuracions insegures en sensors i PLCs per accedir, escalar privilegis o eludir controls d'accés.	IoT, PLCs, endpoints, SCADA.
	T1598 - Phishing for Information	Errors humans	Els atacants utilitzen phishing per recopilar informació valuosa, com credencials, enfocant-se a obtenir dades en lloc d'executar codi maliciós.	Base de dades, Sistemes d'autentificació, xarxes de telecomunicacions , servidors al núvol.
	T1583 - Acquire Infrastructure	Vulnerabilitats al núvol	Adquisició recursos físics o virtuals, com servidors o dominis, per executar activitats malicioses com phishing o DDoS, camuflant-les com trànsit legítim.	Xarxes globals interconnectades , Servidors físics, virtuals i dominis.

Vulnerabilitats Externes	T1557 - Adversary-in-the-Middle	Intercepció de comunicacions	També conegut com el “man in the middle”, els atacants intenten posicionar-se entremig de dos o més dispositius en xarxa explotant la manca de xifrat TLS/SSL en dispositius IoT per obtenir informació valuosa així com per exemple credencials.	IoT, SCADA, Xarxes de telecomunicacions.

Avaluació i priorització de riscos

L'avaluació i priorització de riscos permet determinar quines amenaces són més probables i quin impacte tindran sobre els actius crítics. Aquest procediment assegura que els recursos de l'empresa es distribueixin de manera eficient per mitigar els riscos més rellevants i protegir les operacions generals de l'empresa.

Metodologia aplicada en aquesta secció:

- Una **avaluació qualitativa** mitjançant la **matriu de probabilitat-impacte**.
- Una **avaluació quantitativa**, calculant les pèrdues econòmiques esperades amb mètriques com **ARO** (Annualized Rate of Occurrence), **SLE** (Single Loss Expectancy) i **ALE** (Annualized Loss Expectancy).

Matriu de probabilitat-impacte

La matriu de **probabilitat-impacte** és una eina qualitativa que classifica els riscos segons:

- **Probabilitat**: La possibilitat que l'amenaça es materialitzi (en una escala de 1 a 5).
- **Impacte**: La gravetat de les conseqüències si l'amenaça es materialitza (en una escala d'1 a 5).

Nivell de Risc	Probabilitat	Impacte	Coloració
Alt	4-5	4-5	Vermell (Crític)

Mitjà-Alt	3-4	3-4	Taronja (Important)
Mitjà	2-3	2-3	Groc (Moderat)
Baix	1-2	1-2	Verd (Tolerable)

Matriu de riscos

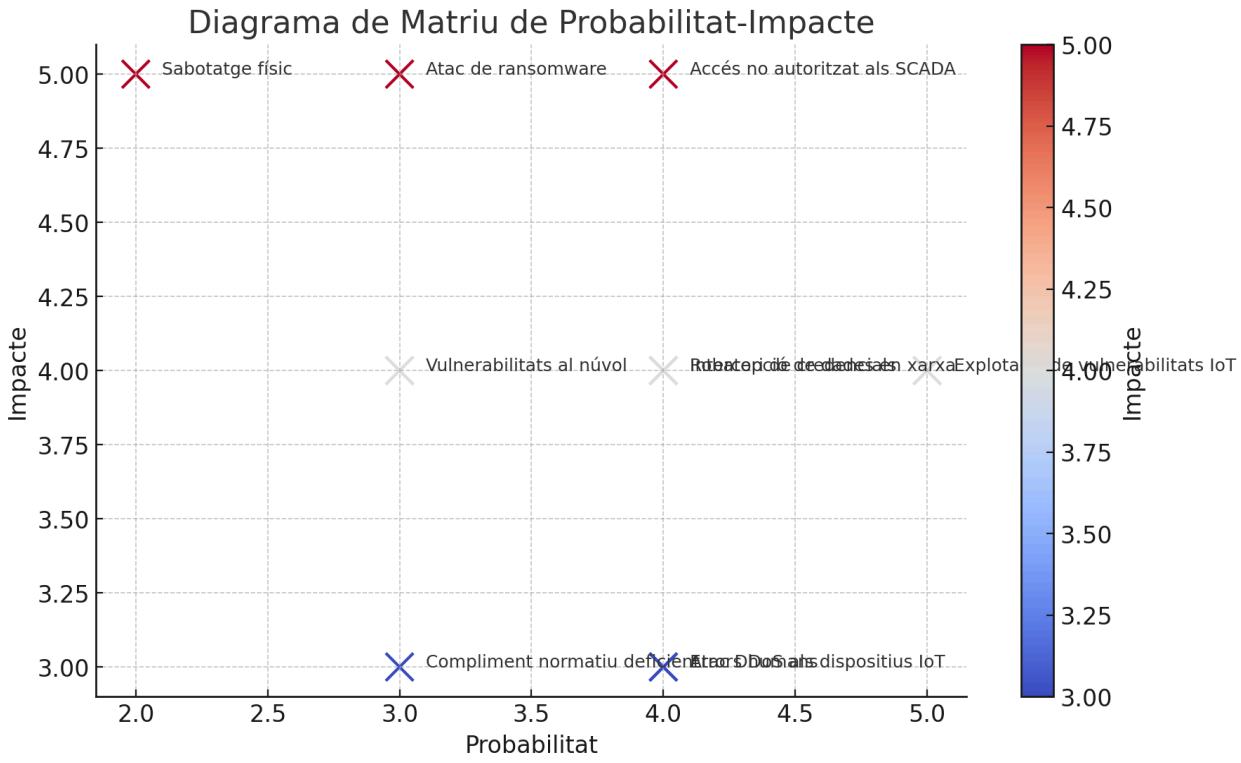
La següent matriu mostra la classificació dels riscos identificats segons la seva **probabilitat** i **impacte**:

Risc	Probabilitat	Impacte	Nivell de Risc
Accés no autoritzat als SCADA	4	5	**Alt**
Atac de ransomware	3	5	**Alt**
Explotació de vulnerabilitats IoT	5	4	**Alt**
Atac DDoS als dispositius IoT	4	3	**Mitjà-Alt**
Intercepció de dades en xarxa	4	4	**Mitjà-Alt**

Sabotatge físic	2	5	**Mitjà-Alt**
Vulnerabilitats al núvol	3	4	**Mitjà**
Errors humans	4	3	**Mitjà**
Robatori de credencials	4	4	**Mitjà-Alt**
Compliment normatiu deficient	3	3	**Mitjà**

Diagrama de matriu de probabilitat-impacte

A continuació es presenta un gràfic de la **matriu de probabilitat-impacte**, que visualitza els riscos en funció de la seva criticitat:



Càlcul econòmic dels riscos prioritaris

Els riscos prioritaris són aquells classificats com a alts en la matriu de probabilitat-impacte. Per aquests riscos, s'ha realitzat una avaluació quantitativa utilitzant les següents fórmules:

- **SLE (Single Loss Expectancy):**
  SLE = Valor de l'Actiu × Percentatge de Pèrdua SLE
  Representa la pèrdua esperada en un sol incident.
- **ARO (Annualized Rate of Occurrence):**
  Nombre d'incidents esperats a l'any.
- ALE (Annualized Loss Expectancy):
  ALE= SLE × AROALE
  Representa la pèrdua econòmica esperada anualitzada.

Exemples:

Risc	Valor de l'actiu	Percentage de perdua	SLE (€)	ARO (Incidents/any)	ALE (€)
Accés no autoritzat als SCADA	1.000.000	50%	500.000	2	1.000.000
Atac de ransomware a les bases dades	800.000	40%	320.000	1	320.000

Justificació de la priorització

Basant-nos en els resultats dels càlculs i la matriu de probabilitat-impacte, els riscos es prioritzen de la següent manera:

- Accés no autoritzat als SCADA
  - **ALE:** 1.000.000 €/any.
  - **Justificació:** L'impacte és crític, ja que pot provocar fallades en el control dels reactors nuclears o altres sistemes industrials. Aquest risc té una elevada probabilitat de ocorrer (ARO = 2).
- Atac de ransomware a les bases de dades
  - **ALE:** 320.000 €/any.
  - **Justificació:** Aquest risc afecta la disponibilitat i integritat de dades crítiques. La seva materialització podria paralitzar operacions clau durant diversos dies, amb costos addicionals per recuperació de dades i multes regulatòries.
- Explotació de vulnerabilitats IoT
  - **Impacte:** Moderat-alt, però amb alta probabilitat (ARO = 5).
  - **Justificació:** Pot interferir greument en el monitoratge d'operacions mitjançant alarmes falses, inoperància de sensors o manipulació de dades. Aquesta explotació pot ser utilitzada com a vector inicial per altres atacs, com el sabotatge.
- Intercepció de dades en xarxa (MitM)
  - **Impacte:** Alt en cas de compromís d'informació sensible.
  - **Justificació:** Pot exposar dades operatives, com claus d'accés i informació estratègica, a actors maliciosos. Aquest risc augmenta la vulnerabilitat davant d'atacs coordinats.
- Atac DDoS als dispositius IoT
  - **Impacte:** Menor des d'un punt de vista econòmic directe, però greu per la seva capacitat d'interferir en les operacions.

- **Justificació:** Aquest risc pot provocar interrupcions prolongades en el monitoratge, especialment en entorns de producció que depenen d'una resposta ràpida a les alertes.

Disseny de controls de seguretat

Introducció al disseny de controls de seguretat

El disseny de controls de seguretat és una etapa fonamental per mitigar els riscos identificats en l'anàlisi anterior. L'objectiu és implementar mesures que protegeixin els actius crítics (IoT, xarxa, núvol i bases de dades) contra les amenaces detectades.

Els controls de seguretat han sigut classificats en tres categories:

- **Controls tècnics:** Són les mesures tecnològiques per prevenir, detectar i respondre als incidents.
- **Controls organitzatius:** Mesures relacionades amb formació del personal, polítiques i estratègies.
- **Controls legals:** Accions per garantir el compliment de les normes i regulacions internacionals.

Controls tècnics

Els controls proposats se separen en tres sectors, els controls tècnics generals, els específics per dispositius IoT i els específics per serveis al núvol.

Controls tècnics generals

Els controls tècnics generals busquen implementar millores tecnològiques que millorin diversos apartats tecnològics per tal d'augmentar la seguretat i disminuir l'impacte i risc d'amenaces en apartats no específics. Aquests controls proposats són:

- **Autenticació robusta:** Implementació d'OAuth o protocols similars.
- **Segmentació de xarxa:** Creació de VLANs per aïllar el tràfic IoT.
- **Monitoratge d'anomalies:** Eines com IDS/IPS per detectar i mitigar intrusions.

- **Actualització regular del firmware:** Gestió mitjançant OTA per eliminar vulnerabilitats.
- **Monitoratge amb Splunk:** Configuració de la plataforma per detectar activitats sospitoses en el trànsit de dades i registres crítics en temps real.
- **Xifratge de dades:** TLS per a trànsit i AES-256 per dades emmagatzemades.
- **Gestió d'usuaris:** Solucions IAM (Identity and access management) per control d'accés i privilegis mínims.

Controls tècnics específics per dispositius IoT

Els dispositius IoT són utilitzats per al monitoratge de reactors nuclears en l'empresa de Neuchâtel-Énergie, els quals són actius importants i vulnerables a atacs.
Els controls proposats són:

- **Gestió centralitzada d'accessos:** Utilització d'un sistema IAM.
- **Xifratge:** Aplicar un xifratge més robust per a dades delicades en trànsit i en repòs.
- **Monitoratge en temps real:** Eines com Splunk per detectar comportaments sospitosos.
- **Auditoria periòdica:** Revisió de configuracions i credencials per defecte.
- **Polítiques de seguretat:** Incloent contrasenyes fortes i autenticació multifactor.

Controls tècnics específics per serveis al núvol

Els controls tècnics per als serveis al núvol tenen com a objectiu protegir la informació crítica emmagatzemada i processada en entorns cloud, augmentant la seguretat i reduint els riscos d'amenaces específiques per aquests serveis. Aquests controls proposats són:

- **Gestió d'identitats i accessos (IAM):** Aplicació de polítiques de mínims privilegis per limitar l'accés només als usuaris autoritzats.
- **Xifratge de dades:** Implementació d'algorismes robustos per protegir la confidencialitat de les dades en trànsit i en repòs.

- **Revisions automatitzades:** Ús d'eines com AWS Config per detectar i corregir configuracions insegures de manera contínua.
- **Monitoratge d'anomalies:** Sistemes com AWS CloudTrail per registrar i identificar activitats sospitoses.
- **Backup i recuperació:** Configuració de còpies de seguretat automatitzades i plans per recuperar dades després d'incidents.

Controls organitzatius

Els controls socials que s'han proposat impliquen accions per conscienciar i educar el personal sobre la ciberseguretat, aquests són:

- **Videovigilància:** Implementació de sistemes de videovigilància avançats, per monitorar zones sensibles de manera contínua i evitar sabotatges.
- **Formació contínua:** Cursos de sensibilització sobre phishing i gestió segura d'informació.
- **Simulacions d'atacs:** Proves regulars per entrenar el personal en la detecció d'amenaces.
- **Programes d'incentius:** Recompenses per identificar i informar sobre vulnerabilitats potencials.

Controls legals

Tal com s'ha dictat anteriorment, l'empresa ha d'assegurar el compliment de les normatives i estàndards internacionals:

- **ISO/IEC 27001:** Implementació d'un SGSI.
- **GDPR:** Garantir la protecció de dades personals dels usuaris i empleats.
- **NERC CIP:** Compliment de regulacions específiques per a infraestructures crítiques en el sector energètic.

- **Auditories externes:** Validació regular per entitats independents per verificar el compliment normatiu.

Taula de correlació entre riscos i controls aplicats

Risc	Control aplicat
Accés no autoritzat als SCADA	Autenticació robusta, segmentació de xarxa (VLAN), formació del personal i compliment de l'estàndard ISO/IEC 27001.
Atac de ransomware	Polítiques de còpies de seguretat, solucions EDR i protocols de resposta a incidents.
Explotació de vulnerabilitats IoT	Segmentació de xarxa, xifrat TLS/SSL, revisió periòdica de firmware i compliment de NERC CIP.
Atac DDoS als dispositius IoT	Monitoratge amb Splunk.
Intercepció de dades en xarxa	Xifratge TLS en comunicacions, simulacions de proves i compliment de ISO/IEC 27001.
Sabotatge físic	Videovigilància amb càmeres Bosch DINION.

Vulnerabilitats al núvol	Xifrat TLS/SSL, monitoratge amb AWS CloudTrail, revisió IAM, i compliment de GDPR i ISO/IEC 27001.
Errors humans	Eines de formació i auditories, sessions de formació continuada i compliment del GDPR.
Robatori de credencials	Monitoratge d'activitats sospitoses amb Splunk.
Compliment normatiu deficient	Simulacions d'incidents, auditories anuals segons normatives ISO/IEC 27001 i NERC CIP.

Simulació i Resposta a Incidents

Descripció del Cas Pràctic: Atac de Ransomware

Context de l'Incident

El 15 de gener de 2025, a les 8:00 del matí, els equips de monitoratge de Neuchâtel-Energie van detectar comportaments anòmals als servidors de bases de dades i al núvol (Azure). Les alertes inicials van indicar un volum inusual de lectures i escrits als arxius crítics, així com intents de connexió a servidors externs desconeguts. A mesura que es va investigar, es va confirmar que una sèrie d'arxius essencials estaven sent xifrats a gran velocitat, una característica dels atacs de ransomware.

Investigació inicial: vector d'entrada

L'origen de l'atac es va rastrejar fins a un **correu electrònic de phishing** enviat a diversos empleats de l'organització. Un membre del departament tècnic va obrir un arxiu adjunt maliciós (un document aparentment legítim), que contenia codi dissenyat per executar el ransomware i iniciar la seva propagació dins de la xarxa.

- **Tècniques utilitzades pel ransomware:**
    - **Execució inicial:** L'arxiu adjunt maliciós aprofitava macros habilitades per executar codi automàticament.
    - **Elevació de privilegis:** El malware explotava vulnerabilitats per obtenir accés administratiu.
    - **Propagació interna:** Mitjançant tècniques com l'escalat lateral (lateral movement) i l'exploració de la xarxa, el ransomware es va expandir ràpidament.

Actius Afectats

L'atac va comprometre actius crítics per al funcionament de les plantes nuclears, provocant un impacte significatiu en les operacions i la seguretat dels reactors nuclears.

Bases de dades crítiques

- **Descripció:** Contenen informació operativa i relativa a la seguretat nuclear, incloent-hi dades sobre els protocols de manteniment dels reactors.
- **Impacte:**
    - La corrupció o pèrdua d'aquestes dades podria:
        - Comprometre la capacitat de gestió dels reactors.
        - Alentitzar decisions crítiques, augmentant el risc d'errors humans o fallades operatives.

Servidors al núvol (Azure i AWS)

- **Descripció:** Emmagatzemen registres d'inspecció, informes tècnics i dades d'operacions essencials per al manteniment diari dels reactors nuclears.
- **Impacte:**
    - La pèrdua d'accés a aquests informes dificulta:
        - L'avaluació de l'estat dels equips.
        - La continuïtat de les operacions, deixant processos crítics sense suport.

Xarxes internes

- **Descripció:** Infraestructura que connecta dispositius i servidors interns.
- **Impacte:**
    - El ransomware es va propagar ràpidament per aquesta xarxa.
        - Impedint la correcta intercomuncació entre les centrals.

- Infectant diversos dispositius i augmentant la dificultat de contenir l'atac.

Impacte de l'Incident

L'atac de ransomware va generar impactes en tres àmbits principals: operatiu, econòmic i reputacional.

Impacte operatiu

L'atac va provocar una **paralització immediata de les operacions crítiques** relacionades amb el manteniment i el monitoratge dels reactors nuclears. Això va suposar:

- **Riscos per a la seguretat operativa i ambiental:**
  - Sense accés a les bases de dades de seguretat i protocols operatius, la capacitat de resposta a situacions crítiques es va veure greument limitada.
  - Es van incrementar els riscos de fallades en els sistemes automatitzats, requerint una major dependència de la intervenció humana, cosa que augmenta la probabilitat d'errors humans.
- **Alentiment en la resposta:**
  - El temps necessari per a la restauració de dades i serveis va dependre de la disponibilitat i la integritat de les còpies de seguretat.
  - Els equips de resposta van necessitar recursos addicionals per contenir i analitzar el malware, retardant la reactivació de sistemes.

Impacte econòmic

L'impacte econòmic de l'incident es va estimar en **300.000 € per hora d'inactivitat**, una xifra que reflecteix la naturalesa crítica de les operacions afectades. Això inclou:

- **Pèrdues associades a la restauració de dades:**

  - Costos per avaluar i verificar còpies de seguretat.
  - Contractació d'equips externs especialitzats en resposta a incidents.
- **Costos d'oportunitat:**
  - Pèrdues generades per la inactivitat dels reactors nuclears.
  - Retards en projectes relacionats amb la gestió i el manteniment preventiu.
- **Inversions futures:**
  - Implementació de noves mesures de seguretat per evitar incidents similars.

Impacte reputacional

L'incident també va afectar la imatge pública de l'organització, especialment pel que fa a la percepció de la seva capacitat per gestionar infraestructures crítiques.

- **Confiança de les agències reguladores:**
  - Les agències reguladores podrien considerar que la gestió de la seguretat nuclear és insuficient, cosa que podria derivar en inspeccions addicionals o sancions.
- **Risc d'exposició pública:**
  - L'atac podria fer-se públic, generant dubtes entre els clients i el públic general sobre la capacitat de l'organització per protegir dades i sistemes sensibles.
- **Impacte en col·laboracions futures:**
  - La percepció negativa podria dificultar col·laboracions amb altres empreses i entitats governamentals.

Pla de Resposta a l'Incident

Aquest pla estructurat consta de quatre fases clau per abordar un incident de seguretat: **Identificació de l'incident**, **Contenció de l'incident**, **Recuperació**, i **Post-anàlisi**.

Aquestes fases estan dissenyades per limitar l'impacte de l'incident, minimitzar el temps d'inactivitat i prevenir futurs casos similars.

Fase 1: Identificació de l'Incident

Objectiu:

Detectar, analitzar i confirmar l'incident per iniciar una resposta ràpida i efectiva, limitant-ne l'impacte i assegurant que es prenen mesures adequades.

Detecció inicial

El procés de detecció comença amb eines automatitzades que monitoren de manera constant la xarxa, els servidors i els dispositius finals. Aquestes eines inclouen:

- **Splunk (SIEM):**
  - Reuneix i analitza dades de logs provinents de múltiples fonts (firewalls, servidors, dispositius finals, etc.).
  - Genera alertes quan detecta comportaments anòmals com xifrat accelerat, canvis de configuració inesperats o connexions a servidors sospitosos.
  - Exemple en el cas pràctic: Splunk va detectar un volum inusual de lectures i escrits als servidors afectats.
- **Palo Alto Firewalls:**
  - Controla el trànsit de xarxa en temps real.
  - Genera alertes per intents de connexió a dominis maliciosos coneguts o patrons de trànsit que s'associen a activitats de ransomware.
- **CrowdStrike Falcon (EDR):**
  - Monitoritzar els dispositius finals per identificar i bloquejar comportaments anòmals, com processos que intenten xifrar molts arxius en poc temps.
  - Exemple en el cas pràctic: CrowdStrike va generar una alarma sobre l'activitat del ransomware a l'ordinador d'un empleat.

- **Alertes dels empleats:**
    - A més de les eines automatitzades, els empleats són instruïts per notificar qualsevol activitat sospitosa, com correus electrònics amb contingut estrany o canvis en l'accés als arxius.

Notificació al CSIRT

Un cop detectada una anomalia significativa, l'incident es comunica immediatament al **Computer Security Incident Response Team (CSIRT)**, que activa el protocol d'emergència. Les accions inclouen:

- **Assignació de responsabilitats:**
    - El CSIRT distribueix tasques específiques a cada membre de l'equip, incloent-hi anàlisi de logs, comunicació amb equips externs i validació de sistemes.
- **Escalament si cal:**
    - Si l'abast inicial de l'incident supera les capacitats internes, el CSIRT pot contactar amb proveïdors externs o equips de resposta a incidents (com Microsoft o Amazon, en aquest cas).
- **Canal de comunicació:**
    - Es crea un canal de comunicació intern dedicat, com un grup segur a Microsoft Teams o Signal, per garantir que les comunicacions siguin ràpides i segures.

Anàlisi preliminar

L'objectiu de l'anàlisi inicial és confirmar la natura de l'incident, determinar-ne l'abast i identificar les prioritats de resposta. Aquest procés inclou:

- **Recopilació de dades:**

  - Splunk correlaciona logs de xarxa, servidors i dispositius finals per identificar el punt d'entrada (en aquest cas, un correu de phishing).
  - Les eines EDR, com CrowdStrike, es fan servir per identificar els fitxers o processos específics responsables de l'atac.
- **Identificació del punt d'entrada:**
  - En el cas pràctic, es detecta que el vector d'atac va ser un correu electrònic amb un arxiu adjunt maliciós descarregat per un empleat del departament tècnic.
- **Determinació de l'abast:**
  - Es verifica quins servidors i dispositius estan afectats. En aquest cas, els servidors Azure, AWS i les bases de dades internes van ser els principals objectius.
  - Es realitza una primera estimació de l'impacte en operacions crítiques.
- **Classificació de l'incident:**
  - Es categoritza l'incident com a **ransomware crític**, i s'assigna una prioritat màxima per iniciar accions immediates.

Confirmació de l'amenaça

Un cop recopilades totes les dades preliminars, es confirma la natura i el comportament de l'amenaça. Aquest pas inclou:

- **Anàlisi del ransomware:**
  - El fitxer sospitós és transferit a un entorn de sandbox per analitzar-ne el comportament.
  - Es determina que es tracta d'una variant de ransomware coneguda (ex.: LockBit o Ryuk), que es propaga per correu electrònic i utilitza tècniques de xifrat robust.
- **Correlació de dades:**

- Les eines de monitoratge (Splunk, CrowdStrike, etc.) es fan servir per identificar patrons comuns a tota la xarxa, confirmant que els servidors afectats han estat objectius de l'amenaça.

- **Creació d'un informe inicial:**
  - Es genera un informe preliminar amb els detalls clau: punts d'entrada, abast inicial, actius afectats i risc potencial.

Fase 2: Contenció de l'Incident

Objectiu:

Limitar l'abast de l'incident per evitar-ne la propagació a altres sistemes i dispositius, garantint que l'impacte es redueixi al mínim possible.

Aïllament immediat dels sistemes afectats

Per evitar la propagació del ransomware, els sistemes compromesos han de ser ràpidament identificats i desconnectats de la xarxa. Les accions concretes inclouen:

- **Desconnexió física i lògica:**
  - Els servidors Azure i les bases de dades internes es desconnecten físicament de la xarxa corporativa i de qualsevol connexió remota (VPN, túnels).
  - Els dispositius finals sospitosos, incloent-hi l'ordinador de l'empleat que va descarregar l'arxiu maliciós, són retirats immediatament.
- **Interrupció de processos maliciosos:**
  - Les eines EDR (com CrowdStrike) es fan servir per identificar i aturar els processos responsables del xifratge en dispositius compromesos.
- **Migració temporal a servidors de contingència:**
  - Els serveis essencials (monitoratge dels reactors nuclears, accés a dades operacionals) es migren a infraestructures de contingència preparades prèviament per mantenir la continuïtat operativa.

Desactivació de les credencials compromeses

Un dels vectors de propagació del ransomware és l'ús d'identitats robades o compromeses. Per mitigar aquest risc:

- **Bloqueig immediat de comptes compromesos:**
  - Es desactiven les credencials de l'empleat que va obrir el correu de phishing, així com qualsevol altre compte amb activitat sospitosa.
- **Monitoratge de l'activitat d'altres comptes:**
  - Es revisen els logs d'autenticació per identificar accessos inusuals o repetits, especialment en comptes amb privilegis elevats.
  - Si es detecten més comptes sospitosos, s'aplica un bloqueig preventiu i es notifica als usuaris afectats.
- **Reforç d'autenticació:**
  - Es força un canvi de contrasenya per a tots els comptes d'usuari, amb requisits de complexitat més estrictes.
  - Es desplega autenticació multifactor (MFA) en tots els accessos als servidors crítics.

Segmentació de la xarxa

La segmentació de la xarxa és essencial per aïllar les àrees compromeses i protegir els actius crítics no afectats. Les accions inclouen:

- **Implementació de VLANs d'aïllament:**
  - Es configuren VLANs específiques per separar els servidors compromesos de la resta de la xarxa corporativa.
  - Els sistemes administratius i d'emmagatzematge crític s'aïllen com a mesura preventiva.
- **Restricció del trànsit de xarxa:**
  - S'utilitzen polítiques de firewalls avançats (NGFW) per bloquejar qualsevol trànsit no essencial entre segments de la xarxa.

- Es desactiva el trànsit cap a dominis maliciosos coneguts, identificats a través de llistes negres actualitzades diàriament.

- **Supervisió activa del trànsit intern:**
  - Es du a terme una anàlisi en temps real de les comunicacions internes per detectar intents de propagació del ransomware.

Anàlisi del ransomware en entorns controlats

Per entendre millor el ransomware i preparar contramesures, es realitza un estudi del fitxer maliciós en un entorn sandbox. Les accions específiques inclouen:

- **Identificació de la variant del ransomware:**
  - Es determina el tipus de ransomware mitjançant eines com Cuckoo Sandbox, VirusTotal o Hybrid Analysis.
  - Exemple: Si es tracta d'una variant coneguda com LockBit, Ryuk o DarkSide, es poden aplicar mesures específiques documentades.
- **Documentació del comportament:**
  - Es monitoritza el comportament del ransomware en l'entorn sandbox, incloent:
    - Fitxers afectats (extensions, directoris).
    - Mètodes de propagació (ex.: ús d'exploits de Windows, credencials robades).
    - Comunicació amb servidors de comandament i control (C2).
- **Generació de contramesures:**
  - A partir de l'anàlisi, es desenvolupen regles personalitzades per als sistemes de detecció i resposta (SIEM, EDR, firewalls).

Coordinació amb equips externs

En incidents d'aquesta magnitud, la col·laboració amb proveïdors i experts externs pot ser clau. Accions inclouen:

- **Contacte amb proveïdors de serveis al núvol:**
    - Es coordinen accions amb Microsoft Azure i AWS per assegurar que els servidors afectats es desconnectin de manera segura i per revisar logs d'activitat sospitosa en els seus sistemes.
- **Col·laboració amb equips de resposta a incidents:**
    - Si l'organització disposa d'un acord amb equips especialitzats (ex.: equips d'IBM X-Force o Mandiant), es notifiquen i es col·laboren en l'anàlisi i contenció.
- **Comunicació amb autoritats reguladores:**
    - Es notifica l'incident a les autoritats competents, especialment si l'impacte afecta infraestructures crítiques o es poden haver exposat dades delicades.

Validació de l'abast de la contenció

Un cop aplicades les mesures de contenció inicials, es verifica que el ransomware ha estat completament aïllat i que no hi ha més propagació. Les accions inclouen:

- **Escanejos exhaustius:**
    - Es fan servir eines com Malwarebytes, Microsoft Defender ATP i l'EDR per buscar rastres del ransomware en dispositius que encara no havien estat afectats.
- **Confirmació del bloqueig de comunicacions externes:**
    - Es revisen les regles dels firewalls i logs de xarxa per assegurar que les connexions amb servidors de comandament i control estan bloquejades.
- **Informe de l'estat actual:**
    - Es genera un informe actualitzat per al CSIRT i les parts interessades, detallant:
        - Sistemes aïllats.
        - Comptes compromesos.
        - Impacte inicial limitat gràcies a les mesures de contenció.

Fase 3: Recuperació

Objectiu:

Restablir els sistemes i serveis afectats garantint la seguretat, integritat i funcionalitat, mentre es minimitza el temps d'inactivitat i es protegeix contra possibles reinfeccions.

Preparació per a la recuperació

Abans d'iniciar la restauració dels sistemes, cal establir un pla clar i assegurar-se que no hi hagi riscos persistents. Les accions inclouen:

- **Validació de l'estat actual:**
  - Es confirma que els sistemes compromesos estan aïllats i que no hi ha propagació activa del ransomware.
  - Es revisen les mesures de contenció aplicades (aïllament, segmentació de xarxa, etc.) per garantir-ne l'efectivitat.
- **Revisió de les còpies de seguretat disponibles:**
  - Es determinen quines còpies de seguretat es poden utilitzar per a la restauració, prioritzant les còpies més recents no afectades.
  - Es verifiquen les còpies amb eines com **VirusTotal**, **Malwarebytes** o **Microsoft Defender ATP** per assegurar que estan lliures de malware.
- **Planificació de la recuperació gradual:**
  - Es desenvolupa un pla per restablir els sistemes en fases, prioritzant els serveis més crítics, com les bases de dades operacionals i els sistemes de monitoratge dels reactors nuclears.

Restauració dels sistemes afectats

La restauració es realitza en diverses etapes per garantir que cada sistema és segur i funcional abans de ser reintegrat a la xarxa. Les accions concretes inclouen:

- **Recuperació de dades des de còpies de seguretat:**
    - Es restauren les bases de dades i servidors des de còpies emmagatzemades en solucions com **Veeam Backup** o equivalents.
    - Es fan proves d'integritat per assegurar que les dades restaurades són completes i correctes.
- **Restauració del sistema operatiu i configuracions:**
    - Els dispositius finals afectats es reconfiguren amb imatges netes de sistemes operatius.
    - Es reinstal·len aplicacions i serveis essencials, amb versions actualitzades que incloguin els últims pegats de seguretat.
- **Recuperació dels sistemes al núvol (Azure i AWS):**
    - Es realitzen restauracions a partir de snapshots segurs prèviament verificats.
    - Els servidors al núvol es reinicien en entorns d'aïllament (sandbox) per assegurar-se que no hi ha presència de codi maliciós abans de la reintegració.
- **Revisió i reparació de configuracions afectades:**
    - Es revisen configuracions de xarxa, comptes d'usuari i regles de seguretat que podrien haver estat alterades durant l'atac.

Validació de la integritat dels sistemes

Abans de reintegrar els sistemes a la xarxa corporativa, cal assegurar-se que estan completament nets i protegits contra futures infeccions. Les accions concretes inclouen:

- **Escanejos exhaustius:**
    - Es fan servir eines com **Malwarebytes EDR**, **CrowdStrike Falcon**, i **Microsoft Defender ATP** per escanejar completament tots els servidors, dispositius i bases de dades restaurats.
- **Simulacions de proves:**

    - Es realitzen simulacions per verificar que els sistemes restaurats responen correctament i que els serveis essencials funcionen sense interrupcions.
- **Monitoratge de trànsit:**
    - Durant aquesta fase, és monitora tot el trànsit de xarxa associat als sistemes restaurats per detectar qualsevol activitat sospitosa.

Reinici gradual dels serveis

La reintegració dels sistemes i serveis es fa de manera controlada per minimitzar el risc d'impactes addicionals. Les accions inclouen:

- **Priorització dels serveis crítics:**
    - Els primers sistemes a restaurar són els relacionats amb el monitoratge i la seguretat dels reactors nuclears.
    - Posteriorment, es reintegren altres serveis operatius i administratius.
- **Aïllament temporal durant la reintegració:**
    - Els sistemes restaurats es mantenen inicialment en entorns segmentats per evitar que puguin interactuar amb altres parts de la xarxa fins que es verifiqui la seva seguretat.
- **Proves de càrrega i funcionalitat:**
    - Es fan proves per assegurar que els servidors i aplicacions poden suportar la càrrega operativa habitual.
- **Validació amb les parts interessades:**
    - Els equips d'operacions i usuaris finals validen que els serveis restaurats compleixen els requisits funcionals i de seguretat.

Fortificació dels sistemes restaurats

Després de la recuperació, es reforcen els sistemes per protegir-los de futures amenaces. Les accions inclouen:

- **Implementació de pegats i actualitzacions:**
  - Es revisen i s'apliquen pegats de seguretat pendents en tots els sistemes.
  - Es comprova que els entorns restaurats utilitzen les últimes versions de les aplicacions i serveis.
- **Millora de configuracions de seguretat:**
  - Es revisen les configuracions de firewalls, regles d'autenticació i permisos d'usuari per evitar possibles vulnerabilitats.
- **Desplegament d'eines addicionals de protecció:**
  - Es consideren solucions addicionals, com sistemes avançats de detecció d'intrusions (IDS/IPS) o solucions de seguretat al núvol (ex.: Azure Security Center).

Comunicació i coordinació amb les parts interessades

Durant tota la fase de recuperació, la comunicació és essencial per mantenir informades totes les parts implicades i coordinar les accions:

- **Notificació als usuaris finals:**
  - Es comunica als empleats quan els serveis tornen a estar operatius i es proporcionen instruccions clares per a l'ús segur dels sistemes restaurats.
- **Informació a la direcció:**
  - L'equip de resposta informa l'equip directiu de l'estat de la recuperació i de les mesures preses per assegurar la continuïtat.
- **Actualització a les autoritats reguladores:**
  - Es proporciona un informe preliminar sobre la restauració i es detallen les mesures de seguretat addicionals implementades.

Fase 4: Post-anàlisi (Lliçons Apreses)

Objectiu:

Documentar tots els detalls de l'incident, identificar-ne les causes arrel i establir accions correctives i preventives per millorar la capacitat de resposta i evitar incidents similars en el futur.

Anàlisi de la causa arrel (Root Cause Analysis)

Aquest pas és fonamental per identificar com es va originar l'incident i establir mesures específiques per evitar que es repeteixi. Les accions concretes inclouen:

- **Revisió del vector d'entrada:**
  - Es confirma que el vector d'entrada va ser un correu electrònic de phishing amb un arxiu adjunt maliciós.
  - Es fa una auditoria completa del correu electrònic, incloent-hi:
    - Tipus d'arxiu adjunt (ex.: un document PDF o Word amb macros malicioses).
    - Característiques del correu (ex.: redacció sospitosa, domini del remitent).
- **Traçabilitat de l'atac:**
  - Es reconstrueix el recorregut del ransomware dins la xarxa per identificar els punts febles explotats.
  - Exemple: si l'empleat afectat tenia accés a servidors crítics, es revisen les polítiques de permisos i segmentació de la xarxa.
- **Anàlisi de vulnerabilitats:**
  - Es revisen les configuracions dels sistemes compromesos per identificar vulnerabilitats, com:
    - Absència d'actualitzacions o pegats de seguretat.
    - Configuracions insegures de comptes o contrasenyes.

- Manca de segmentació adequada a la xarxa.

Revisió i millora dels controls de seguretat

A partir de les causes arrel identificades, es millora les defenses de l'organització. Les accions inclouen:

- **Actualització dels sistemes de detecció:**
  - Es milloren les configuracions del **SIEM** (Splunk) i les eines EDR (CrowdStrike) per detectar més ràpidament patrons associats a ransomware.
  - Es creen regles específiques per bloquejar variants conegudes del ransomware identificat.
- **Fortificació dels correus electrònics:**
  - Implementació d'eines avançades de protecció, com **Barracuda Email Security Gateway** o **Proofpoint**.
  - Configuració de filtres de correu electrònic per bloquejar:
    - Arxius adjunts sospitosos (ex.: extensions no habituals).
    - Dominis de remitents desconeguts o maliciosos.
- **Revisió de polítiques de seguretat:**
  - Es reforcen les polítiques d'accés basat en privilegis mínims (principle of least privilege).
  - S'implementen requisits més estrictes per a les contrasenyes i s'assegura que tots els comptes utilitzen **autenticació multifactor (MFA).**
- **Segmentació de la xarxa:**
  - S'implementen polítiques de segmentació més estrictes (VLANs) per limitar l'accés entre diferents parts de la xarxa.
  - Es revisa la configuració del **Next-Generation Firewall (NGFW)** per bloquejar trànsit sospitós en temps real.

Formació i sensibilització del personal

Els empleats són una de les primeres línies de defensa contra atacs com el phishing. Les accions per millorar la seva preparació inclouen:

- **Sessions de formació periòdiques:**
  - Programes educatius sobre ciberhigiene i bones pràctiques.
  - Enfocament en la detecció de correus sospitosos i la gestió segura d'arxius adjunts.
- **Simulacions d'atacs:**
  - Es realitzen simulacions regulars de phishing per avaluar la resposta dels empleats i identificar punts de millora.
  - S'ofereixen sessions de formació personalitzades per als empleats que mostrin mancances en la detecció de phishing.
- **Cultura de seguretat:**
  - S'estimula una cultura proactiva en què els empleats se sentin segurs informant sobre possibles amenaces o activitats sospitoses.

Informe complet de l'incident

L'equip **CSIRT** redacta un informe detallat que documenta tots els aspectes de l'incident. Aquest informe serveix tant com a registre històric com a guia per a futurs plans de resposta. Els punts inclouen:

- **Cronologia de l'incident:**
  - Descripció detallada dels esdeveniments, des de la detecció fins a la recuperació.
  - Exemple: "8:00 AM: Splunk genera una alerta d'activitat anòmala al servidor Azure. 8:15 AM: CrowdStrike identifica un procés de xifrat als servidors."
- **Impacte operatiu i econòmic:**
  - Estimació de les pèrdues econòmiques:

        - Temps d'inactivitat total x cost estimat (ex.: 300.000 €/hora).
    - Descripció de l'impacte operatiu en serveis essencials (ex.: retard en el monitoratge dels reactors nuclears).
- **Actius afectats:**
    - Llista detallada de sistemes compromesos i les accions preses per restaurar-los.
- **Accions de contenció i recuperació:**
    - Resum de les mesures implementades en cada fase de resposta.
- **Recomanacions per al futur:**
    - Accions específiques per millorar les defenses i la preparació de l'organització.

Avaluació del temps de resposta i eficiència

Un cop completat l'informe, es revisen les mètriques clau per avaluar l'efectivitat del pla de resposta:

- **Temps de resposta:**
    - Es compara el temps transcorregut en cada fase amb els objectius establerts (ex.: temps de detecció, contenció i recuperació).
- **Eficàcia de les eines:**
    - Es revisen les capacitats de les eines utilitzades (SIEM, EDR, firewalls) i es proposen millores si cal.
- **Rendiment de l'equip:**
    - Es fa una revisió interna del rendiment de l'equip CSIRT per identificar punts de millora.

Comunicació amb les parts externes

Finalment, es gestiona la comunicació amb entitats externes per assegurar la transparència i protegir la reputació de l'organització:

- **Informació a autoritats reguladores:**
    - Es proporciona un informe complet i es demostren les accions correctives implementades.
- **Gestió de la reputació:**
    - Si hi ha risc d'exposició pública, es prepara un comunicat de premsa que expliqui l'incident i les mesures preses per evitar futurs problemes

Conclusions

L'anàlisi de riscos realitzat a Neuchâtel-Énergie ha permès identificar i abordar de manera exhaustiva les principals amenaces i vulnerabilitats als quals s'enfronten els actius crítics d'aquesta empresa. Aquest procés s'ha desenvolupat seguint una metodologia rigorosa basada en estàndards reconeguts internacionalment com l'ISO/IEC 27001 i el NIST Cybersecurity Framework, així com en bones pràctiques específiques del sector nuclear.

Principals resultats de l'anàlisi:

- **Identificació i classificació d'actius:**
  - S'ha creat un inventari complet que inclou tant actius físics (sensors IoT, sistemes SCADA, servidors locals) com lògics (bases de dades, aplicacions IoT, serveis al núvol).
  - Els actius han estat classificats segons el seu impacte potencial i prioritat, destacant aquells directament vinculats a la seguretat dels reactors nuclears.
- **Identificació i anàlisi de riscos:**
  - S'han documentat amenaces crítiques com ara l'accés no autoritzat als sistemes SCADA, atacs de ransomware dirigits a bases de dades delicades i explotacions de vulnerabilitats en dispositius IoT.
  - L'anàlisi també ha evidenciat debilitats internes com errors humans i configuracions inadequades, així com riscos externs com atacs avançats i desastres naturals.
- **Avaluació i priorització dels riscos:**
  - Mitjançant eines com la matriu de probabilitat-impacte, s'han prioritzat els riscos més crítics segons el seu impacte econòmic i operatiu.
  - L'avaluació quantitativa (SLE, ARO, ALE) ha estimat pèrdues anuals potencials significatives, i això permet justificar la implementació de controls específics.

- **Proposta de controls de seguretat:**
    - S'han recomanat mesures tècniques, com el xifratge TLS/SSL, segmentació de xarxes i implementació d'IDS/IPS per protegir els actius identificats.
    - En l'àmbit organitzatiu, s'ha proposat la formació continuada del personal i el desenvolupament de protocols estrictes de gestió d'incidents.
- **Simulació d'un atac i resposta:**
    - S'ha simulat un atac de ransomware afectant bases de dades crítiques, validant l'efectivitat d'un pla de resposta estructurat en quatre fases: identificació, contenció, recuperació i post-anàlisi.
    - La restauració ràpida de dades mitjançant còpies de seguretat ha minimitzat els impactes operatius i econòmics.

Limitacions i reptes futurs:

Tot i que l'anàlisi ha estat exhaustiva, s'han identificat diverses limitacions relacionades amb la dependència de dades teòriques, la variabilitat de les amenaces i els costos associats a la implementació de controls avançats. Per afrontar aquests reptes, es recomana dur a terme auditories periòdiques, millorar els plans de resposta a incidents i invertir tant en tecnologia com en formació continuada del personal.

En conclusió, aquest projecte ha brindat una perspectiva completa dels riscos cibernètics vinculats a la companyia nuclear, Neuchâtel-Énergie, fonamentant una base sòlida per salvaguardar la seva infraestructura vital i afavorint la resistència operativa i ciberseguretat en un sector tan delicat.

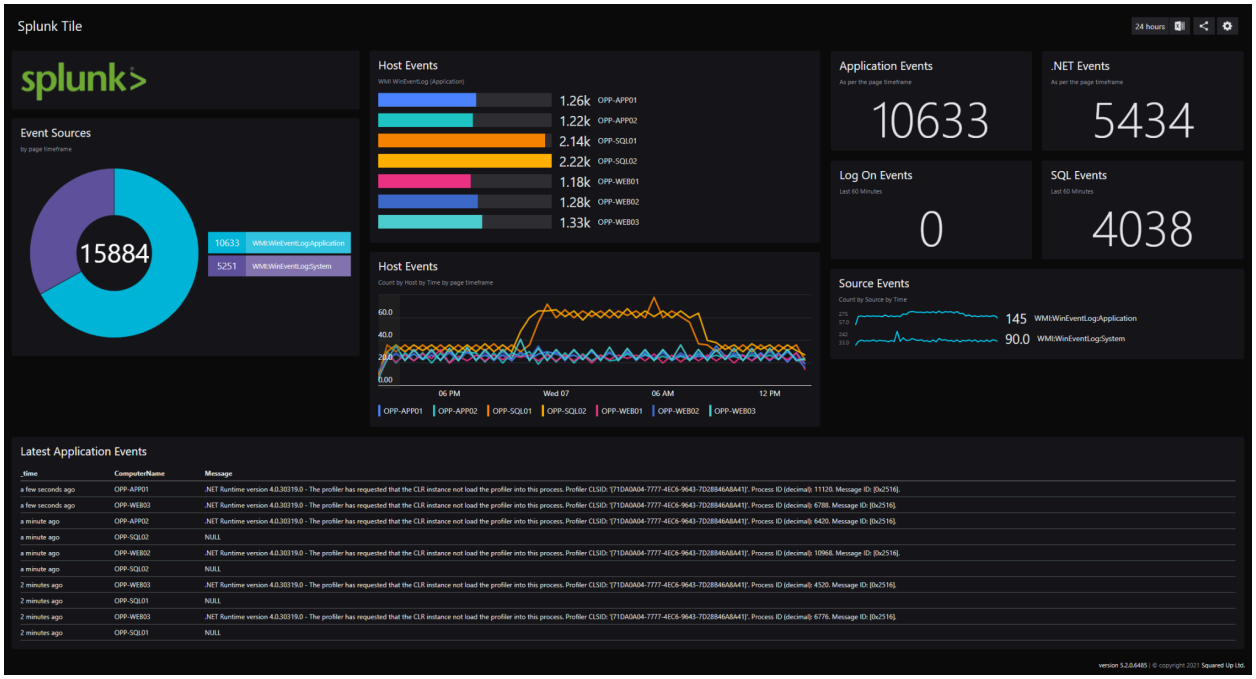
Annexos

Annex 1: Captures de pantalla de sistemes i eines utilitzades

A continuació es presenten captures de pantalla d'eines utilitzades en l'anàlisi de riscos, configuració de sistemes i detecció d'incidents.

Eina de monitoratge i detecció d'incidents: Splunk

- Splunk s'ha utilitzat per a la **detecció d'activitat sospitosa** en xarxes internes i dispositius connectats (SCADA, IoT).



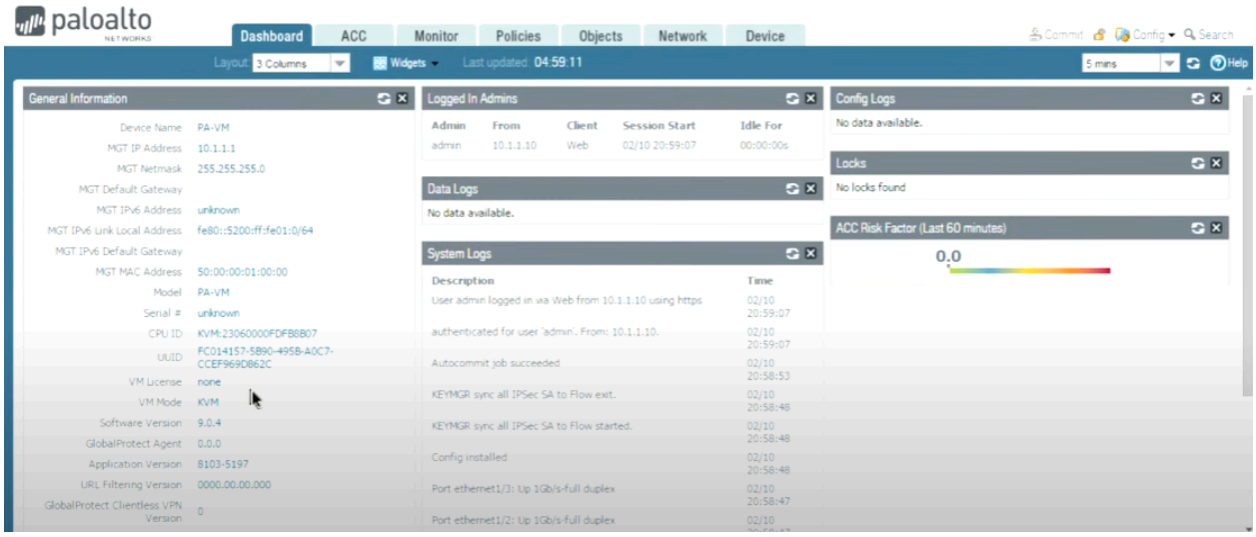
Configuració de firewalls avançats: Palo Alto NGFW

- Configuració d'un **Next-Generation Firewall** per bloquejar tràfic no autoritzat entre VLANs i protegir dispositius IoT.

Configuració exemple:

set rulebase security rules "IoT_Sensors_Block" from "untrust" to "trust"

source "any" destination "IoT_vlan" application "any" action "deny"



Configuració de xifratge TLS/SSL

- Implementació de **xifratge TLS/SSL** en dispositius IoT i comunicacions SCADA per protegir dades en trànsit.

Configuració exemple:

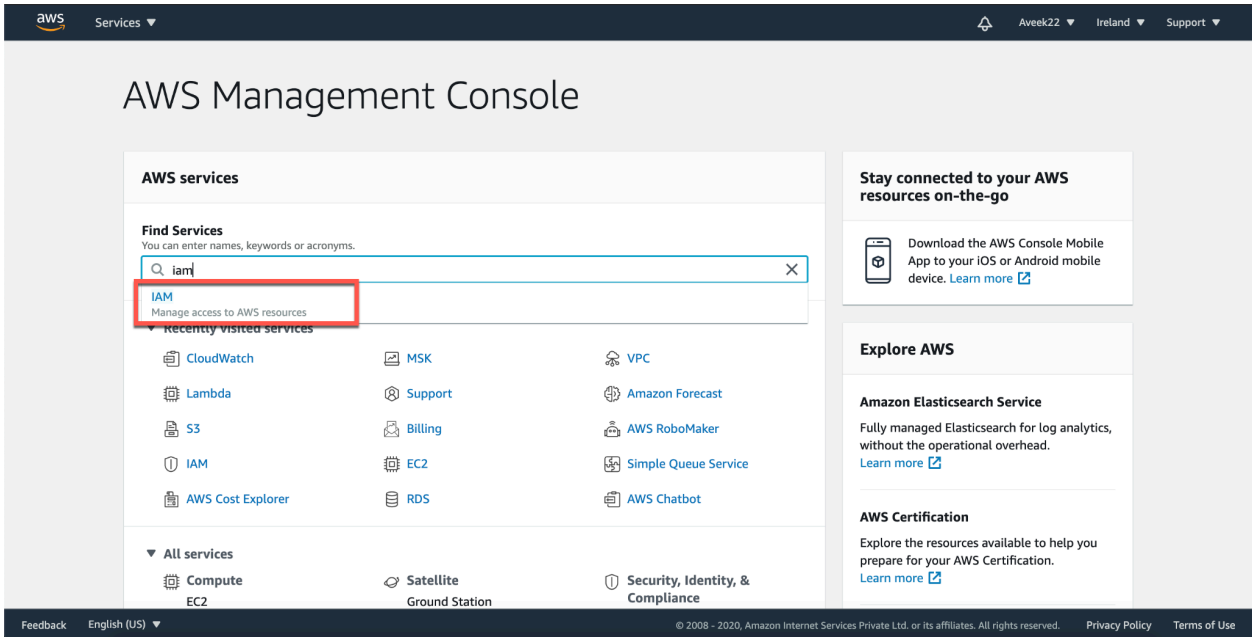
openssl req -new -x509 -days 365 -key iotserver.key -out iotserver.crt

dbConnect

	Name	Data type	Start value
1	Static		
2	Secure	TCON_IP_V4_SEC	
3	ConnPara	TCON_IP_v4	
4	InterfaceId	HW_ANY	0
5	ID	CONN_OUC	256
6	ConnectionType	Byte	16#0B
7	ActiveEstablished	Bool	true
8	RemoteAddress	IP_V4	
9	ADDR	Array[1..4] of Byte	
10	ADDR[1]	Byte	192
11	ADDR[2]	Byte	168
12	ADDR[3]	Byte	12
13	ADDR[4]	Byte	83
14	RemotePort	UInt	8080
15	LocalPort	UInt	2000
16	ActivateSecureConn	Bool	true
17	TLSServerReqClientCert	Bool	false
18	ExtTLSCapabilities	Word	16#0
19	TLSServerCertRef	UDInt	2
20	TLSClientCertRef	UDInt	3

Configuració d'IAM a AWS

Creació de rols IAM per aplicar el principi de **mínims privilegis** en servidors al núvol.



Annex 2: Normatives aplicades en l'anàlisi

Normativa	Descripció
ISO/IEC 27001	Estàndard internacional per a la gestió de la seguretat de la informació.
NIST Cybersecurity Framework	Marc de bones pràctiques per millorar la resiliència cibernètica.
GDPR (Reglament UE 2016/679)	Regulació sobre la protecció de dades personals dins la Unió Europea.

NERC CIP	Normes específiques per protegir infraestructures crítiques del sector energètic.
NIST SP 800-30	Guia per a l'anàlisi i gestió de riscos en sistemes informàtics.

Annex 3: Documentació tècnica

Taula de correlació entre riscos i controls aplicats *(Resum complementari)*

Risc	**Control tècnic**	**Control organitzatiu**	**Control normatiu**
Accés no autoritzat als SCADA	Autenticació robusta, VLAN	Formació del personal	ISO/IEC 27001
Atac de ransomware	Polítiques de backup, EDR	Protocols de resposta a incidents	NIST Cybersecurity Framework
Vulnerabilitats IoT	Segmentació de xarxa, TLS/SSL	Revisió periòdica de firmware	NERC CIP
Errors humans	Eines de formació, auditories	Sessions de formació continuada	GDPR

Intercepció de dades en xarxa	Xifratge de comunicacions (TLS)	Simulacions de proves	ISO/IEC 27001

Annex 4: Configuració bàsica de resposta a incidents

Procediment resumit de resposta a incidents (NIST SP 800-61):

Fase	Accions realitzades
Identificació	Detecció amb Splunk, confirmació amb anàlisi forense i informes dels logs.
Contenció	Aïllament dels servidors afectats, bloqueig d'usuaris i tràfic sospitós.
Recuperació	Restauració de dades des de còpies de seguretat i verificació d'integritat.
Post-anàlisi	Informe de l'incident, actualització de polítiques i millora de controls existents.

Bibliografia

1. ISO/IEC 27001:2022. (2022). *International Organization for Standardization.*
2. National Institute of Standards and Technology (NIST). (2012). *NIST SP 800-30 Rev 1.*
3. European Commission. (2016). *General Data Protection Regulation (GDPR).*
4. NERC. (2019). *Critical Infrastructure Protection (CIP) Standards.*
5. Cisco Systems. (2021). *Next-Generation Firewalls: Implementació i Seguretat.*
6. AWS Security Best Practices. (2023). *Amazon Web Services Documentation.*
7. Splunk Inc. (2023). *Using Splunk for Incident Detection and Response.*
8. Siemens. (2023). *IoT Security for Industrial Systems.*

Normatives i estàndards

1. **ISO/IEC 27001:2022** (Gestió de la Seguretat de la Informació):
    - ISO/IEC 27001 - International Organization for Standardization
2. **NIST Cybersecurity Framework** (Marc de Ciberseguretat):
    - NIST Cybersecurity Framework
3. **NIST SP 800-30 Rev. 1** (Guia per a l'anàlisi de riscos):
    - NIST SP 800-30 - Risk Management Guide
4. **General Data Protection Regulation (GDPR)** (Protecció de dades):
    - Reglament General de Protecció de Dades - GDPR
5. **NERC CIP** (Seguretat en infraestructures crítiques energètiques):
    - NERC CIP Standards

Eines tècniques

6. **Splunk** (Monitoratge i anàlisi de logs):
    - Splunk - Plataforma de Detecció i Monitoratge
7. **Palo Alto Networks - NGFW** (Next-Generation Firewall):
    - Palo Alto Networks Firewalls

8. **AWS Cloud Security** (Pràctiques de seguretat en Amazon Web Services):
    - AWS Security Best Practices
9. **Azure Security** (Microsoft Azure):
    - Microsoft Azure Security Best Practices
10. **Siemens Industrial IoT Security**:
    - Siemens MindSphere - IoT Security
11. **Veeam Backup & Replication** (Còpies de seguretat):
    - Veeam - Solucions de Backup
12. **CrowdStrike Falcon** (Endpoint Detection and Response - EDR):
    - CrowdStrike Falcon EDR

Documentació de referència

13. **AWS IAM Policies** (Gestió d'identitats i accessos):
    - AWS Identity and Access Management
14. **TLS/SSL Encryption Configuration**:
    - Configuració TLS/SSL a OpenSSL
15. **Cisco Systems - Xarxes Segures**:
    - Cisco Security Solutions
16. **ABB Ability System 800xA** (Sistemes SCADA):
    - ABB Ability System 800xA
17. **Yokogawa IoT Monitoring** (Sensors de pressió industrial):
    - Yokogawa - EJA530E Sensors
18. **Honeywell Radiation Monitors**:
    - Honeywell RadEye SPRD

Referències generals de ciberseguretat

19. **National Cyber Security Centre (NCSC)**:
    - NCSC Cyber Security Guidance
20. **OWASP IoT Project** (Pràctiques de seguretat per dispositius IoT):
    - OWASP IoT Security

21. **CIS Controls** (Center for Internet Security):
    - CIS Controls for Cyber Defense

Altres enllaços útils

22. **MITRE ATT&CK Framework** (Models d'amenaces):
    - MITRE ATT&CK
23. **Cybersecurity and Infrastructure Security Agency (CISA)**:
    - CISA Resource Center

Enllaços a components

24. **Energiforsk. (2021). Industrial Internet of Things in Nuclear**
    - https://energiforsk.se/media/29219/industrial-internet-of-things-in-nuclear-energiforskrapport-2021-726.pdf
25. **U.S. Nuclear Regulatory Commission. (2006).**
    - https://www.nrc.gov/docs/ML0635/ML063530382.pdf
26. **Encardio-Rite Electronics Pvt. Ltd. (n.d.).**
    - https://www.encardio.com/blog/nuclear-power-plant-sensors-and-condition-monitoring
27. **Mycle Schneider Consulting. (n.d.). World Nuclear Industry Status Report: Reactors.**
    - https://www.worldnuclearreport.org/reactors.html#tab=iso
28. **Yokogawa Electric Corporation. (n.d.). General Specifications: Field Control Station.**
    - https://web-material3.yokogawa.com/GS01C31F01-01EN.pdf
29. **Bosch Security Systems. (n.d.).**
    - https://resources-boschsecurity-cdn.azureedge.net/public/documents/DINION_5100i_IR__Data_sheet_enUS_105250134283.pdf
30. **Schneider Electric. (n.d.). Ecodial Advanced Calculation: Software Overview.**

- https://download.schneider-electric.com/files?p_Doc_Ref=DIA6ED2151012EN&p_enDocType=Catalog&p_File_Name=DIA6ED2151012EN.pdf

31. **Cisco Systems, Inc. (n.d.).**
    - https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.pdf
32. **Palo Alto Networks. (n.d.).**
    - https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/es_ES/resources/datasheets/pa-5200-series
33. **Siemens. (n.d.). MindSphere:**
    - https://www.plm.automation.siemens.com/media/global/en/Siemens-MindSphere-Whitepaper-69993_tcm27-29087.pdf
34. **Splunk. (n.d.). Splunk Enterprise.**
    - https://www.splunk.com/en_us/products/splunk-enterprise.html