1.)

Firstly, security should be planned from the start. In the end, this will be the most cost effective option to ensure the required security level in the power plants. This might mean identifying the most important parts of the system to protect and give extra emphasis on those. Also, potential attackers' viewpoint can be considered in order to find the possible entrypoints in the system.

Security should also be implemented into each part of the process from coding and testing to release of the software. Security tests can be applied during coding and one of the tests can be a simulated attack.

Even though the software might be thoroughly tested, new exploits are continuously found. Thus, preparing for incidents is necessary. The company should have a plan in cases of attacks or failures to ensure the stability in the critical parts of the system. In cases of disaster, they should have planned ways to recover as much as possible. Backing up data for example goes without saying.

After all this, there should be regular security reviews to ensure the security standards are up to date in the software. New exploits should be patched when found and the team should be aware of the new exploits and attacks in the field.

2.)

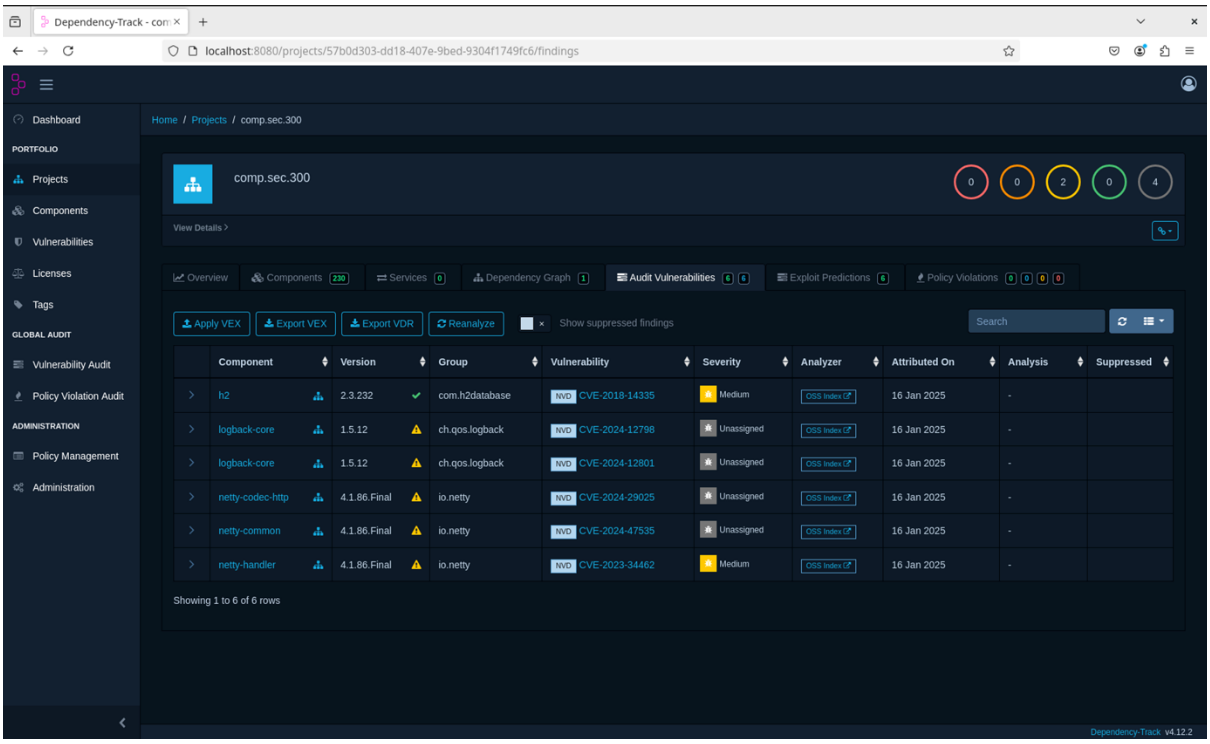
i. BOM.json is in the other attachments

ii.

```
ubuntu@primary:~/dependency-track$ mvn org.cyclonedx:cyclonedx-maven-plugin:makeAggregateBom
[INFO] Scanning for projects...
[INFO]
[INFO] ----------------< org.dependencytrack:dependency-track >----------------
[INFO] Building Dependency-Track 4.13.0-SNAPSHOT
[INFO] --------------------------------[ war ]---------------------------------
[INFO]
[INFO] --- cyclonedx-maven-plugin:2.9.1:makeAggregateBom (default-cli) @ dependency-track ---
[INFO] CycloneDX: Resolving Dependencies
Downloading from ossrh-snapshot: https://oss.sonatype.org/content/repositories/snapshots/junit/junit-dep/maven-metadata.xml
[INFO] CycloneDX: Creating BOM version 1.5 with 230 component(s)
[INFO] CycloneDX: Writing and validating BOM (JSON): /home/ubuntu/dependency-track/target/bom.json
[INFO]          attaching as dependency-track-4.13.0-SNAPSHOT-cyclonedx.json
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  6.609 s
[INFO] Finished at: 2025-01-16T15:23:51+02:00
[INFO] ------------------------------------------------------------------------
```

```
ubuntu@primary:~/dependency-track$ sudo docker ps -a
CONTAINER ID   IMAGE                      COMMAND                CREATED            STATUS
PORTS                          NAMES
02e9f8e468c0   dependencytrack/frontend    "/docker-entrypoint.…"   About an hour ago   Up 7
minutes          0.0.0.0:8080->8080/tcp, :::8080->8080/tcp     ubuntu-dtrack-frontend-1
9d0e8c0b6378   dependencytrack/apiserver    "/bin/sh -c 'exec ja…"   About an hour ago   Up 7
minutes (healthy)   0.0.0.0:8081->8080/tcp, [::]:8081->8080/tcp   ubuntu-dtrack-apiserver-1
```

iii.



	Component	Version		Group	Vulnerability	Severity	Analyzer	Attributed On	Analysis	Suppressed
›	h2	2.3.232	✓	com.h2database	NVD CVE-2018-14335	Medium	OSS Index	16 Jan 2025	-	
›	logback-core	1.5.12	⚠	ch.qos.logback	NVD CVE-2024-12798	Unassigned	OSS Index	16 Jan 2025	-	
›	logback-core	1.5.12	⚠	ch.qos.logback	NVD CVE-2024-12801	Unassigned	OSS Index	16 Jan 2025	-	
›	netty-codec-http	4.1.86.Final	⚠	io.netty	NVD CVE-2024-29025	Unassigned	OSS Index	16 Jan 2025	-	
›	netty-common	4.1.86.Final	⚠	io.netty	NVD CVE-2024-47535	Unassigned	OSS Index	16 Jan 2025	-	
›	netty-handler	4.1.86.Final	⚠	io.netty	NVD CVE-2023-34462	Medium	OSS Index	16 Jan 2025	-	

Showing 1 to 6 of 6 rows

h2: CVE-2018-14335
severity: Medium
An issue was discovered in H2 1.4.197. Insecure handling of permissions in the backup function allows attackers to read sensitive files (outside of their permissions)
via a symlink to a fake database file.

logback-core: CVE-2024-12798
severity: Unassigned

ACE vulnerability in JaninoEventEvaluator by QOS.CH logback-core
upto including version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 in Java applications allows attacker to execute arbitrary code by compromising an existing logback configuration file or by injecting an environment variable before program execution.

logback-core: CVE-2024-12801
severity: Unassigned
Server-Side Request Forgery (SSRF) in SaxEventRecorder by QOS.CH logback version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 on the Java platform, allows an attacker to forge requests by compromising logback configuration files in XML.
The attacks involves the modification of DOCTYPE declaration in XML configuration files.

netty-codec-http: CVE-2024-29025
severity: Unassigned
Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients.
The `HttpPostRequestDecoder` can be tricked to accumulate data.
While the decoder can store items on the disk if configured so, there are no limits to the number of fields the form can have, an attacher can send
a chunked post consisting of many small fields that will be accumulated in the `bodyListHttpData` list.
The decoder cumulates bytes in the `undecodedChunk` buffer until it can decode a field, this field can cumulate data without limits.
This vulnerability is fixed in 4.1.108.Final.

netty-common: CVE-2024-47535
severity: Unassigned
Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients.
An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty
attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crashes.
This vulnerability is fixed in 4.1.115.

netty-handler: CVE-2023-34462
severity: Medium
Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients.
The `SniHandler` can allocate up to 16MB of heap for each channel during the TLS handshake. When the handler or the channel does not have an idle
timeout, it can be used to make a TCP server using the `SniHandler` to allocate 16MB of heap.
The `SniHandler` class is a handler that waits for the TLS handshake to configure a `SslHandler` according to the indicated server name by the `ClientHello` record.

For this matter it allocates a `ByteBuf` using the value defined in the `ClientHello` record.
Normally the value of the packet should be smaller than the handshake packet but there are not checks done here and the way the code is written,
it is possible to craft a packet that makes the `SslClientHelloHandler`. This vulnerability has been fixed in version 4.1.94.Final.

iv.

```
ubuntu@primary:~/dependency-track$ mvn org.cyclonedx:cyclonedx-maven-plugin:makeAggregateBom
[INFO] Scanning for projects...
[INFO]
[INFO] ----------------< org.dependencytrack:dependency-track >----------------
[INFO] Building Dependency-Track 4.13.0-SNAPSHOT
[INFO] --------------------------------[ war ]---------------------------------
[INFO]
[INFO] --- cyclonedx-maven-plugin:2.9.1:makeAggregateBom (default-cli) @ dependency-track ---
[INFO] CycloneDX: Resolving Dependencies
Downloading from ossrh-snapshot: https://oss.sonatype.org/content/repositories/snapshots/dummy/dummy/1.0/dummy-1.0.pom
Downloading from central: https://repo.maven.apache.org/maven2/dummy/dummy/1.0/dummy-1.0.pom
[WARNING] The POM for dummy:dummy:jar:1.0 is missing, no dependency information available
Downloading from ossrh-snapshot: https://oss.sonatype.org/content/repositories/snapshots/junit/junit-dep/maven-metadata.xml
Downloading from ossrh-snapshot: https://oss.sonatype.org/content/repositories/snapshots/dummy/dummy/1.0/dummy-1.0.jar
Downloading from central: https://repo.maven.apache.org/maven2/dummy/dummy/1.0/dummy-1.0.jar
[WARNING] Unable to create Maven project for dummy:dummy:jar:1.0 from repository.
[INFO] CycloneDX: Creating BOM version 1.5 with 231 component(s)
[INFO] CycloneDX: Writing and validating BOM (JSON): /home/ubuntu/dependency-track/target/bom.json
[INFO]          attaching as dependency-track-4.13.0-SNAPSHOT-cyclonedx.json
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  5.925 s
[INFO] Finished at: 2025-01-16T17:08:34+02:00
[INFO] ------------------------------------------------------------------------

ubuntu@primary:~/dependency-track$ cat target/bom.json | jq '.components[] | select(.name=="dummy")'
{
  "type": "library",
  "bom-ref": "pkg:maven/dummy/dummy@1.0?type=jar",
  "group": "dummy",
  "name": "dummy",
  "version": "1.0",
  "scope": "required",
  "purl": "pkg:maven/dummy/dummy@1.0?type=jar"
}
```