WÄRTSILÄ PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT) PROCESS

Providing vulnerability advisory and incident response

1. INCIDENT REPORTING
   Customer contacts Wärtsilä via existing channels, Wärtsilä contacts PSIRT

2. PREPARATION
   Preparing the environment to support effective incident response by enabling the collection of forensics data

3. IDENTIFICATION
   Defining incident validity from related data (e.g. logs and error messages)
   - Valid
   - Not valid

4. CONTAINMENT
   Limiting the damage and isolating systems to prevent further damage (e.g. isolating the infected system components)

5. RECOVERY
   Implementing controls (e.g. patching) at affected site and bringing systems back online

6. LESSONS LEARNED
   Completion of the incident documentation for continuous improvement

7. ERADICATION
   Finding the incident’s root cause and removing the malware (e.g. by patching, hardening, other controls) to prevent the incident to reoccur

PSIRT BENEFITS:

- Detects threats before they turn to incidents or damages
- Detects and resolves incidents and keeps business ongoing without interruptions
- Offers incident response service to support incident handling
- Addresses security vulnerabilities and proposes mitigating actions