ENERGI CERT

Handbook on Threat Assessments

October 2022

TLP:CLEAR

Table of contents

ENERGI CERT

Introduction

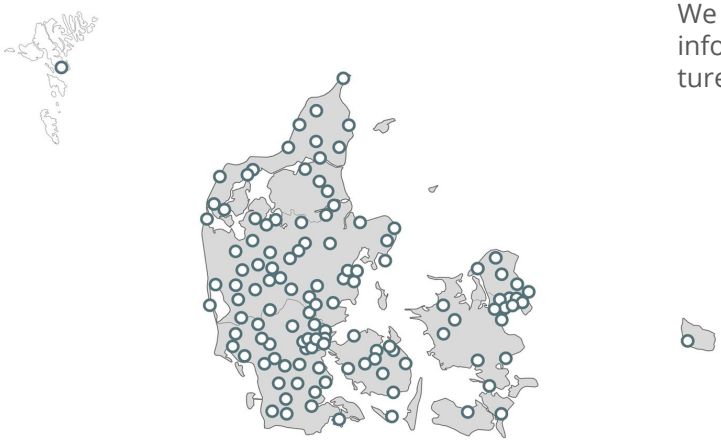
About EnergiCERT

EnergiCERT is the critical sectors' cyber security centre.

EnergiCERT is an essential part of the sectors' defence against cyber threats. We help detect and respond to cyber-attacks on critical infrastructure, and build and share the critical knowledge that can prevent the next attack.

Our responsibilities include monitoring the companies in the sectors that are connected to our extensive sensor network. Through the sensor network, we monitor Internet traffic in order to detect cyber attacks against Danish critical infrastructure.

EnergiCERT is a non-profit association owned and funded by Danish companies in the critical infrastructure sector. We cooperate with other CERTs in Europe and are part of a number of cyber security organisations, which gives us a high level of knowledge about the threats to critical infrastructure.



ENERGI CERT

About the handbook

This handbook describes the framework for EnergiCERT's assessment of the current cyber threat to Danish critical infrastructure companies. The current assessment will always be available on the EnergiCERT website.

The handbook is produced by EnergiCERT and shared with EnergiCERT members, authorities and other interested parties.

The handbook can with advantage be used by EnergiCERT members to understand the current level and to be prepared to navigate the different threat levels. One way to prepare is to follow the recommendations of EnergiCERT, including the general recommendations provided in this handbook.

One of the elements of the EnergiCERT threat assessment is a sensor network and a network of honeypots operated by EnergiCERT. The sensor network covers approximately 200 companies and ensures that EnergiCERT is always aware of cyber attacks currently attempted against critical infrastructure in Denmark.

We use this information - along with other information that enriches the threat picture - to form our threat assessments.

Classification

EnergiCERT uses Traffic Light Protocol (TLP) version 2 when sharing information to specify how the information can be shared further. Note that TLP version 2 is new (August 2022).

The TLP scale is divided into four levels as shown in the picture. Each level indicates whether and to what extent the information may be shared. The restrictions on sharing apply both to the sharing of the actual document and to other oral and written communication of the content.

This document is classified as TLP:CLEAR, which means that the information can be shared freely.

Learn more about the Traffic Light Protocol at FIRST: www.first.org/tlp/.

TLP:**RED**
The information is solely intended for the recipient as a person.

TLP:**AMBER**
The information can be shared internally within the recipient's own organisation as well as with companies or individuals who receive cyber security services from the recipient's organisation.
When TLP:**AMBER+STRICT** is used, it means that the information may only be shared internally within the recipient's organisation.

TLP:**GREEN**
The information can be shared freely within the relevant community. A community could be "Danish energy companies".

TLP:**CLEAR**
The information can be shared indefinitely.

ENERGI CERT

THREAT ASSESSMENT

Introduction to EnergiCERT threat assessment and threat levels.

EnergiCERT threat levels

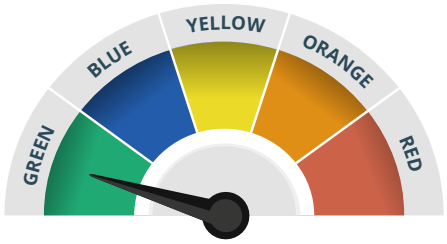
Objective
The objective of the EnergiCERT threat assessment is to inform Danish actors in the critical sectors about the current cyber threat against them.

EnergiCERT's threat assessment should be seen as complementary to other information on the threat picture that each actor may possess. The overall picture thus becomes part of the basis for the actors' own cyber security risk assessments.

International standard
EnergiCERT works to an international standard of threat levels. The standard was developed by the Center for Internet Security (CIS) and is called "Alert Level Information". By using this standard, EnergiCERT can ensure that threat levels can be widely understood among both members and collaborators.

5 levels
The standard contains 5 levels and goes from green (normal image) to red (highest level).

Visualization
EnergiCERT displays the current threat level via a graphical element as shown here. The purpose is for stakeholders to quickly see the current level and understand where on the scale the level belongs.



Publication of threat level
As a stakeholder, you should always be aware of the current threat level. When EnergiCERT assesses that the cyber threat is changing, this will be made public through the various member channels and via the website.

EnergiCERT will explain why we are changing levels and elaborate on which technical and organisational recommendations we think you should focus on validating. These recommendations will draw from the list of recommendations on page 17 and will be based on the current threat.

How to read and apply the threat levels
Each threat level is described in the following sections. For each level, a brief description of the level is provided, as well as various recommendations:

- *Extraordinary measures*, are actions that EnergiCERT recommends being performed at this threat level.
- *Validation of security level*, refers to the additional focus on validating the effectiveness of the security measures mentioned.
- *Reporting*, indicates what should be focused on by reporting and the frequency of this reporting.
- *Change of frequency*, indicates examples of areas where the frequency of execution of the task should be adapted to the current threat picture.

In addition, the description of each level also tells what can be expected from EnergiCERT.

Proper preparation is essential

Recommendations for critical infrastructure actors

EnergiCERT has - based on our knowledge of both actors and our knowledge of cybersecurity in critical infrastructure - made 25 recommendations for technical and organisational measures. These 25 recommendations are all ones we strongly recommend all actors to have implemented regardless of the threat level we are at. These are listed in the Preparation section on page 17.

Validation

When EnergiCERT changes to a new threat level - whether up or down - we will also list, along with information on the threat level, those of the 25 recommendations we think you should pay extra attention to validating the impact of. This means that we recommend that you check whether the measures in question are working as expected.

For example, one recommendation could be to validate that your patch management is working. This means that you make checks to ensure that your systems are actually patched, that the patches are installed correctly, that the systems are rebooted and that all this happens within the time period you have defined in your patch policy.

Recommendations

EnergiCERT is not an authority and therefore cannot require an actor to act on a particular threat level.
These are recommendations - not requirements.

Coordination

In developing the threat levels and recommendations, EnergiCERT has coordinated with relevant government agencies, Center for Cybersikkerhed and PET, and has had a thorough dialogue with our members.

Can threat levels be assessed differently?

There are many people other than EnergiCERT who make threat assessments and recommendations, including the Center for Cybersikkerhed.

It is important to note that different standards may be used so that threat levels do not mean the same thing. For example, EnergiCERT's highest level (RED) will be used very rarely - and even in these cases, very briefly.

EnergiCERT assesses both the threat (what we expect to happen), the factual (what is actually happening) and our knowledge of the resilience of Danish critical infrastructure actors and combines this into one threat level.

This means, for example, that we can go up in threat level if there is a serious attack against some systems that we know are used in the sectors and for which there is no patch right now. It also means that when the patch comes and we expect the sectors to have installed it, we will go down in threat level because the risk of being hit is much lower.

This contrasts with many others who provide threat assessments, as another view of this may be that the threat is still the same even if the patch is installed.

DESCRIPTION OF THREAT LEVELS

This describes each threat level and the recommendations that go with it.
This can be used both as a reference when changing to a new threat level and to prepare for what is expected of you when threat levels change.
The threat levels are also presented in one consolidated table in the Appendix.

Threat level GREEN

The following apply

- No unusual activity other than known hacking activities, malware and other malicious activity not expected to affect critical infrastructure.

Recommendations for critical infrastructure actors

Extraordinary measures

- Be sure to actively participate in SektorForum. Share all incidents, threats, etc. against critical infrastructure as well as information on changes in threat picture.
- Make sure your EnergiCERT contact point is up to date.

Validation of security level

By switch to this threat level, EnergiCERT will provide concrete recommendations (see page 17) on which protection measures you should validate are working as intended.

This will be announced on the SektorForum and in other communications provided by EnergiCERT in connection with the change to this threat level.

Reporting

- Internal reporting to management on the status of security and preparedness at least annually.
- We encourage stakeholders - according to their own assessment of needs - to report on the status of implementation of recommendations as well as identified incidents (via SektorForum).

Change of frequency

Do what you usually do to make sure your environment is safe.

Maintain the frequency of patching, log analysis, review of controls, review of vendor security, etc. that you have defined in your security policies.

What to expect from EnergiCERT

- Follows normal processes
- Projects are implemented as planned
- Follows normal sharing process.

Communication

- Webinar on why the threat level has changed (within 5 days).

Threat level BLUE

At least one of the following applies

- There is an indication of a general risk of serious hacking activity, malware or other malicious activity.
- While there is potential for malicious cyber activity, EnergiCERT does not see cyber activity among its members that is likely to cause an impact on critical infrastructure.
- We see an increase in attack attempts or a change in attack types.

Recommendations for critical infrastructure actors

Extraordinary measures

All extraordinary measures from threat level GREEN must be carried out and in addition:

- Engage with your suppliers to explain why the threat picture has changed and make sure they are following your level of preparedness.

Validation of security level

By switch to this threat level, EnergiCERT will provide concrete recommendations (see page 17) on which protection measures you should validate are working as intended.

This will be announced on SektorForum and in other communications provided by EnergiCERT in connection with the change to this threat level.

Reporting

- Internal reporting to management on the status of security and preparedness at least quarterly.
- We encourage stakeholders - according to their own assessment of needs - to report on the status of implementation of recommendations as well as identified incidents (via SektorForum).

Change of frequency

What you usually do to make sure your environment is safe, you now need to do a little more often.

Increase your frequency of patching, log analysis, review of controls, review of vendor security, etc.

What to expect from EnergiCERT

- Follows normal processes
- Projects are implemented as planned
- Follows normal sharing process
- Focus on the current threat.

Communication

- Webinar on why the threat level has changed (within 5 days).

Threat level YELLOW

At least one of the following applies

- Indicates a significant risk of serious hacking activity, malware or other malicious activity.
- There is a concrete threat to Danish companies and EnergiCERT sees cyber activities among its members that have the potential to affect critical infrastructure.
- We see vulnerabilities in critical infrastructure being successfully exploited against other countries, where we assess that the same would work against Danish companies.

Recommendations for critical infrastructure actors

Extraordinary measures

All extraordinary measures from threat level BLUE must be carried out and in addition:

- Conduct a contingency exercise to test your contingency plan against the current threat
- Prepare to operate in island mode (simulation).

Validation of security level

By switch to this threat level, EnergiCERT will provide concrete recommendations (see page 17) on which protection measures you should validate are working as intended.

This will be announced on SektorForum and in other communications provided by EnergiCERT in connection with the change to this threat level.

Reporting

- Internal reporting to management on the status of security and preparedness at least monthly.
- We encourage stakeholders to report on the status of implementation of recommendations as well as identified incidents on a weekly basis (via SektorForum).

Change of frequency

What you usually do to make sure your environment is safe, you now need to do more often.

There is a need for more frequent (than at threat level BLUE) patching, log analysis, review of controls, review of security of suppliers, etc.

Threat level YELLOW

What to expect from EnergiCERT

- Review of normal tasks and projects to assess whether staff should be removed from these to join the contingency
- Weekly 15 min briefings with the team
- Communication is prioritised and the sharing process intensified
- Focus on the current threat.

Communikation

- Webinar on why the threat level has changed. This will be conducted as soon as possible during normal working hours
- More frequent sharing of information
- Publication of situation reports if we stay in YELLOW for a longer period.

Also pay attention to

Pay extra attention to employees' well-being and that they can switch off completely to ensure that they are able to stay focused for longer periods of time.

Threat level ORANGE

At least one of the following applies

- Indicates a high risk of serious hacking activity, malware or other malicious activity targeting critical infrastructure.
- There is a concrete, verified threat to Danish companies that EnergiCERT has seen attempted used and where there is potential for impact on critical infrastructure.
- EnergiCERT sees persistent, direct, targeted attack attempts (or previously unseen attack types) against members that may either directly or indirectly affect critical infrastructure.

Recommendations for critical infrastructure actors

Extraordinary measures

All extraordinary measures from threat level YELLOW must be carried out and in addition:

- Activate crisis response as described in your contingency plans.
- Go into limited island mode: limit or disconnect network connections that are not necessary for the continued operation of essential services.

Validation of security level

By switch to this threat level, EnergiCERT will provide concrete recommendations (see page 17) on which protection measures you should validate are working as intended.

This will be announced on SeKtorForum and in other communications provided by EnergiCERT in connection with the change to this threat level.

Reporting

- Internal reporting to management on the status of security and preparedness at least weekly.
- We encourage stakeholders to report on a daily basis on the status of implementation of recommendations and identified incidents (via SektorForum).

Change of frequency

What you usually do to make sure your environment is safe, you now need to do even more often.

A much more frequent frequency (than at lower threat levels) is needed for patching, log analysis, review of controls, review of security of suppliers, etc.

Threat level ORANGE

What to expect from EnergiCERT

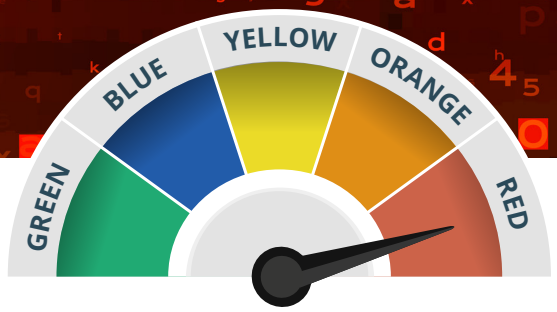
- All normal tasks and projects are put on hold and everyone is part of the contingency
- Daily 15 min briefings with the team
- We test satellite phones, SINE radios, Starlink connections and generators as we go to ORANGE threat level
- Communication is prioritised and the sharing process intensified
- Focus on the current threat
- EnergyCERT prioritises the interests of society over those of individual companies.

Communikation

- Webinar on why the threat level has changed. This is done as soon as possible, regardless of
- time.
- More frequent sharing of information
- Monthly calls become weekly calls
- Publication of situation reports.

Also be aware of

Establish a contingency plan to ensure that people get sleep and that on-call staff are replaced regularly.



Threat level RED

At least one of the following applies

- Indicates a very high risk of serious hacking activity, malware or other malicious activity that could affect the entire Danish society.
- EnergiCERT sees serious attacks against members' critical infrastructure and there is a serious risk that large parts of society's critical infrastructure will be affected.
- There is a crisis at national level.

Recommendations for critical infrastructure actors

Extraordinary measures

All extraordinary actions from threat level ORANGE must be performed and in addition:

- Use alternative communication methods, e.g. satellite phone or SINE radio.
- Enter island mode to ensure the continued operation of critical infrastructure.
- Activate emergency procedures.
- Call in all relevant staff ("all hands on deck").

Validation of the security level

By switch to this threat level, EnergiCERT will provide concrete recommendations (see page 17) on which protection measures you should validate are working as intended.

This will be announced on SektorForum and in other communications provided by EnergiCERT in connection with the change to this threat level.

Reporting

- Internal reporting to management on the status of security and preparedness at least daily.
- We encourage stakeholders to continuously report on the status of implementation of recommendations as well as identified incidents (via SektorForum or available channels such as satellite phone, SINE radio or other).

Change of frequency

Increase your frequency for patching, log analysis, review of controls, review of security with vendors etc. so that it is now done continuously.

Note that when operating in island mode, changes to that part of the infrastructure should be kept to a minimum.

Threat level RED

What to expect from EnergiCERT

- All normal tasks and projects are put on hold and everyone is part of the contingency
- All hands on deck (war room)
- Planned holidays likely to be postponed
- Daily 15 min briefings with the team
- We test satellite phones, SINE radios and Starlink connections once a week
- We test generators when we go to RED threat level
- Communication is prioritised and the sharing process intensified
- Focus on the current threat
- EnergiCERT prioritises the interests of society over those of individual companies.

Communication

- Webinar on why the threat level has changed. This is done as soon as possible, regardless of
- time
- More frequent sharing of information
- Monthly calls become weekly calls or daily calls
- Publishing of situation reports.

Also be aware of

Establish a contingency plan to ensure that people get sleep and that on-call staff are replaced regularly.

PREPARATION - 25 RECOMMENDATIONS

EnergiCERT has developed 25 concrete recommendations for critical infrastructure actors, which we recommend are implemented regardless of the threat level we are in.

Recommendations

EnergiCERT has developed a list of 25 concrete actions that we recommend all critical infrastructure actors to implement.

Good OT and IT security

It is important to stress that this is not an exhaustive list, but should be seen as a set of minimum recommendations that all critical infrastructure actors should implement in the view of EnergiCERT.

Preparation

Implementation should be independent of the current threat level, as it would be too late to start implementing these measures once the need arises.
The list of recommendations should therefore be seen as an opportunity to check that either all the recommendations have already been implemented - or to refocus on getting the missing recommendations implemented.

Use SektorForum

If you need sparring on good ways to implement the recommendations, you can use the SektorForum, where both we in EnergiCERT and your colleagues in other critical infrastructure companies can be found.

Recommendations

1 Firewall
Firewall is implemented and kept up to date - preferably with geo-blocking of countries not needed to receive traffic from.

2 Exposure of services
Only absolutely necessary services are exposed to the Internet.

3 Endpoint protection
Endpoint protection and firewall enabled and updated on all systems.

4 Backup
Backup is present (including off-site backup) and restore is tested regularly.

5 Password length
Passwords are designed according to current standards - i.e. rather very long passwords that are changed rarely than shorter passwords that are changed frequently.

6 No password reuse
No password reuse across IT and OT.

7 No shared logins and default passwords
No common login and no default passwords.

8 Remove inactive users
User accounts that are not used are removed or disabled.

9 Multifactor validation
All services with login exposed to the Internet are secured with multifactor validation and remote access is limited as much as possible.

10 Update
The systems are kept up to date / patched - including third-party software.

11 Identify outdated systems
Vulnerable systems that cannot be patched (end-of-life e.g.) are identified and appropriate countermeasures are implemented to protect them.

12 Contingency plan
A contingency plan is drawn up and maintained.

13 Log collection
Monitoring / logging implemented so that attacks can be detected and responded to in a timely manner - e.g. via EnergiCERT sensors, honeypots on the OT network and extended, internal monitoring.

ENERGI CERT

Recommendations

14 Awareness
Awareness training of employees is conducted on an ongoing basis to ensure focus on OT and IT security.

15 Map network entries
All network entries to the production network are mapped.

16 Segmentation
The network is segmented into several layers - at least so that OT is separated from IT. Consider further isolation or segmentation to contain or limit the potential of an incident.

17 Identify devices
All units in the production environment are identified and documented.

18 Documentation
Both logical and physical documentation of the architecture is produced.

19 Limit rights
Limiting rights on user accounts - special focus on limiting administrative rights for users when not necessary.

20 Access policy
Policy on access to the production network is established.

21 Policy for changes
Policy for changes to the digital part of the production network is established.

22 Vendor management
Vendor management policy, including how to verify that vendors meet your security requirements, is established.

23 Alternative communication channels
Alternative communication methods, e.g. satellite phone or SINE radio to complement e-mail and telephone, are established.

24 Emergency procedures
Emergency procedures for all business-critical processes are drawn up so that the function can be performed in the event of prolonged IT outages, including a plan for operation in island mode.

25 Vulnerability Scans
Ongoing vulnerability scans and possibly penetration tests are conducted to provide an overview of the attack surface towards the Internet.

APPENDIX

The same information described above about threat levels, recommendations, and what to expect from EnergiCERT is presented here in a table to easily compare the differences between threat levels.

Threat levels

	GREEN	BLUE	YELLOW	ORANGE	RED
Description of threat levels	No unusual activity other than known hacking activities, malware and other malicious activity not expected to affect critical infrastructure.	Indicates a general risk of serious hacking activity, malware or other malicious activity. *or* There is potential for harmful cyber activities, but EnergiCERT does not see cyber activities among its members that are likely to cause an impact on critical infrastructure. *or* We see an increase in attack attempts or a change in attack types.	Indicates a significant risk of serious hacking activity, malware or other malicious activity. *or* There is a concrete threat to Danish companies and EnergiCERT sees cyber activities among its members that have the potential to affect critical infrastructure. *or* We see vulnerabilities in critical infrastructure being successfully exploited against other countries where we assess that the same would work against Danish companies.	Indicates a high risk of serious hacking activity, malware or other malicious activity targeting critical infrastructure. *or* There is a concrete, verified threat to Danish companies that EnergiCERT has seen attempted use and where there is potential for impact on critical infrastructure. *or* EnergiCERT sees persistent, direct, targeted attack attempts (or previously unseen attack types) against members that may either directly or indirectly affect critical infrastructure.	Indicates a very high risk of serious hacking activity, malware or other malicious activity that could affect the entire Danish society. *or* EnergiCERT sees serious attacks against members' critical infrastructure and there is a serious risk that large parts of society's critical infrastructure will be affected. *or* There is a crisis at national level.

How EnergiCERT acts

	GREEN	BLUE	YELLOW	ORANGE	RED
How EnergiCERT acts	Follows normal processes. Projects are being implemented as planned. Follows normal sharing process.	Follows normal processes. Projects are being implemented as planned. Follows normal sharing process. Focus on the current threat.	Review of normal tasks and projects to assess whether staff should be removed from these to join the contingency. Weekly 15 min briefings with the team. Communication is prioritised and the sharing process intensified. Focus on the current threat.	All normal tasks and projects are put on hold and everyone is on standby Daily 15 min briefings with the team We are exceptionally testing satellite phones, SINE radios and Starlink connections as we go to ORANGE threat level Communication is prioritised and the sharing process intensified Focus on the current threat EnergiCERT prioritises the interests of society over those of individual companies	All normal tasks and projects are put on hold and everyone is on standby All hands on deck (war room) Planned holidays likely to be postponed Daily 15 min briefings with the team We test satellite phones, SINE radios and Starlink connections once a week We test generators when we go to RED alert Communication is prioritised and the sharing process intensified Focus on the current threat EnergiCERT prioritises the interests of society over those of individual companies
Communikation from EnergiCERT	Webinar on why the threat level has changed (within 5 days)	Webinar on why the threat level has changed (within 5 days)	Webinar on why the threat level has changed. This will be done as soon as possible during normal working hours More frequent sharing of information Publication of situation reports if we stay in YELLOW for a longer period	Webinar on why the threat level has changed. This will be done as soon as possible, regardless of time More frequent sharing of information Monthly calls become weekly calls Publication of situation reports	Webinar on why the threat level has changed. This will be done as soon as possible, regardless of time More frequent sharing of information Monthly calls become weekly or daily calls Publication of situation reports

Recommendations to operators

	GREEN	BLUE	YELLOW	ORANGE	RED
Extraordinary measures	Be sure to actively participate in SektorForum. Share all incidents, threats, etc. against critical infrastructure as well as information on changes in the threat picture. Verify that the EnergiCERT's contact point at your site is updated.	**Everything from GREEN as well as:** Engage with your suppliers to explain why the threat picture has changed and make sure they are following your level of preparedness	**Everything from BLUE as well as:** Conduct a contingency exercise to test your contingency plan against the current threat Prepare to operate in island mode (simulation)	**Everything from YELLOW as well as:** Activate crisis response Enter limited island mode: limit or disconnect network connections that are not necessary for the continued operation of essential services.	**Everything from ORANGE as well as:** Enter island mode to ensure the continued operation of critical infrastructure Use alternative communication methods, such as satellite phone or SINE radio Activate emergency procedures Call in all employees ("all hands on deck")
Coordination		**Ad-hoc / as needed** We encourage stakeholders - according to their own assessment of needs - to report on the status of implementation of recommendations as well as identified incidents (via SektorForum).	**Weekly** We encourage stakeholders to report on the status of implementation of recommendations as well as identified incidents on a weekly basis (via SektorForum).	**Daily** We encourage stakeholders to report on the status of implementation of recommendations as well as identified incidents on a daily basis (via SektorForum).	**By the hour** We encourage stakeholders to continuously report on the status of implementation of recommendations as well as identified incidents (via SektorForum or available channels such as satellite phone, SINE radio or other).
Change of frequency E.g. patch frequency, log analysis, review of controls, review of security of suppliers, etc.	**Normal**	**Increased**	**Often**	**Very often**	**Continuous** *Note that when operating in island mode, changes to that part of the infrastructure should be kept to a minimum.*
Internal reporting to management on the state of security and preparedness	**Minimum annually**	**Minimum quarterly**	**Minimum monthly**	**Minimum weekly**	**Daily**

Recommendations to operators

	GREEN	BLUE	YELLOW	ORANGE	RED
Focus on validation of safety level.	When switching to this threat level, EnergiCERT will provide concrete recommendations (see page 17) on which protection measures you should validate are working as intended. This will be announced on SektorForum and in the other communications provided by EnergiCERT in connection with the change to this threat level.				
Plan to be in this threat level for this period		Years	Months	Weeks	Days
Considerations in relation to this			Pay extra attention to employees' well-being and that they can switch off completely to ensure that they are able to stay focused for a longer period of time.	Establish a contingency plan to ensure that people get sleep and that on-call staff are replaced regularly	Establish a contingency plan to ensure that people get sleep and that on-call staff are replaced regularly

Contact us

Contact EnergyCERT at the following number:

+45 88327140

If you have any questions about EnergiCERT, you are also welcome to send an email:

info@energicert.dk

PGP nøgle:

86B4 C9C8 5C53 513C 1D8F 6F14 B877 3115 64F5 AE13

Visiting and postal address:

Sommerfuglevej 2A
6000 Kolding

CVR number:

41369841

Satellite phone:

+88 1622456029