Q&A of Cyber Tips webinar 'Incident Handling: From Chaos To Control'

By CCB Connect & Share

CENTRE FOR CYBERSECURITY BELGIUM

#	Question	Answer
1	When does a case qualify to get help from the Cert?	As Sebastien just mentioned, our main constituents are NIS2 entities. While we would love to be able to support everyone, unfortunately, that's not possible with our limited resources. We will try to help as much as possible though.
2	So I understand it is a free service offered to anyone who falls under NIS2? (follow-up of question 'When does a case qualify to get help from the Cert?')	The service offered by the CCB is always free, regardles of whether the organisation falls under NIS2 or not.
3	How many ransomware and DDoS attacks were reported last month?	In May 2025, CCB was informed of 9 new ransomware cases. When it comes to DDoS attacks, we had 4 reported incidents but we would like to stress that this not a realistic represention of DDoS attacks in Belgium. Often organisations that have efficient solutions against DDoS attacks, hardly or don't even notice that they are being attacked. There are several intel providers that provide DDoS reports which give more insight when it comes to DDoS attacks. Like this report for example: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/
4	NIS2 entity here. I heard we should contact the local police department first on an incident, and they would contact the CCB/CERT. Is that correct or should we contact you directly with the form?	This is incorrect information, you would need to report the incident directly to the CCB. Since this is related to legal obligations as a NIS2 entity, we would like to refer you to the following link: https://atwork.safeonweb.be/nl/nis2. Here you will also find a guide how to report an incident (https://ccb.belgium.be/sites/default/files/2024-11/NIS2_Notification_guide_10-2024_v1.2-NL.pdf). In general, you do not need to go through the police to submit a NIS2 notification, but in case of an intrusion, we do advise filing a complaint as well. See also section 3.3.4 of our NIS2 FAQ (https://ccb.belgium.be/sites/default/files/2025-02/NIS2%20FAQ%20Website%20v2.0.1%20EN.pdf).
5	A few questions related to DDoS attacks: How do you detect/identify DDoS attacks on Belgian companies? How do you help organizations handle these? How do you contact the impacted company? (e.g. the case of Roularta earlier this month)	On a daily basis our dedicated team of CTI analysts parses through data and alerts we find pertaining to Belgian organizations. While we cannot give details on the how and where, this involves an extensive set of monitoring tools. Whenever we find information on an organization in Belgium that is or is about to be the victim of a cyber attack we reach out to them via phone or by mail. Our analysts use contact details from our databases or contact information we find online. If you register at SafeOnWeb@Work, that contact information will also be used to reach out to your organization. At the initial contact we make an assessment of severity and level of request for help, depending on the help requested different responses can be offered. This can range from sharing IOCs, offering advice, to the escalation to the CERT team. The method to communicate further will be agreed upon based on the preferences of the victim organization.
6	And how can we stay in touch? What are the preferred ways to communicate in such cases?	Initial contact is best done by either phone or the webform: https://notif.safeonweb.be/nl. After that you can tell us the best ways to reach you for future communication.
7	Does reporting an incident to CCB qualify reporting to government from a compliance perspective?	More information on NIS2 guidelines and obligations can be found here: https://atwork.safeonweb.be/nl/nis2
8	Do you have a dataset publicly available which demonstrates the type of industries involved in cybersecurity incidents notified to CCB/Cert?	This is currently not publicly available.

9	Is the CyFun label mandatory to show compliance? Can we use our ISO 27001 certification? What if the ISO 27001 scope does not cover the full organisation? thanks!	The label is not mandatory but a tool to demonstrate that the ISO27001 certificate is in line with NIS2/CyFun. An ISO27001 certificate that is valid for a scope that does not cover the whole entity is unlikely to be compliant with NIS2
10	What if the ISO 27001 certification is not delivered by a CAB ?	then it is not a valid certification to fullfill the requirements for essential entities
11	What is the most dangerous threat: phishing, a virus, or something else?	That really depends on the situation and is not so straightforward. Phishing is also a broad term that can encompass many different types of phishing, some more harmfull than others. When it comes to preparedness there really is no substitution for an all-around approach. Keep your users informed of possible phishing threats whilst keeping your systems up to date, checking for known vulnerabilities and threats.
12	Currently, in the context of DORA, we are required to notify the FSMA, and potentially also the DPA (GBA) and CCB in case of an incident. Do you know if there are any plans to streamline this process in the future, for example through a single point of contact or platform?	DORA is legislation that quaifies as lex specialis as mentioned in art. 6 of the NIS2 law. Therefore, art. 6 §§3-4 stipulate that the security measure and reporting obligations (art. 30-65) do not apply to DORA entities. Nevertheless, the National Bank and FSMA forwards notifications received to CCB.
13	In case we're compromised where CCB can help? Technical? Support on site? Tx Ronny	Our incident response services range from expert advice to full on forensic investigation and incident handling. This sometimes is done remotely if the situation allows or on-site if needed.
14	Do you also have a communication plan in case of a cyber attack?	Here you can find tips and guidelines on how to prepare your crisis communication plan: https://atwork.safeonweb.be/crisis-communication-event-cyber-attack
15	In all incident cases you managed, could you give the percentage on how many were "on premise infrastructure" versus cloud infrastructure?	A percentage is hard to give, you also need to keep in mind here that a lot of organizations work in a hybrid setup. In such a setup you might see attacker activity on both. But it is clear that the cloud is a big attack surface these days.
16	Can we test the report form without submitting it? https://ccb.belgium.be/cert/report-incident	We would recommend to test the report form and submit it with 'TEST' clearly mentioned in the subject. This way we know it's a test and we can confirm to you if the test report was well received without taking any further action.
17	Any view on when this year the CyFun model be adapted to NIST CSF 2.0 ? :)	Barring unforeseen circumstances, CyFun® 2025 and accompanying materials will be available in at the end of Q3 - beginning of Q4.
18	Recently, Microsoft blocked the email account of the chief prosecutor of the International Criminal Court (ICC), Karim Khan, due to US sanctions. If it happened to Belgian institutions or belgian-based proeminent organisations, would the CCB have a strategy in such cases? Would it qualify as “cyber-Incident”?"	It could potentially qualify as a NIS2 incident, if it has an impact that reaches the thresholds specified in the NIS2 guide. If you need access to your email to properly provide your NIS2 services, and not having access to them anymore could be a serious operation disruption, then yes, it could qualify as a NIS2 incident. Besides, losing access to your email might also be a loss of personal data, but that's a GDPR issue.
19	Would you still recommend a FIDO key as MFA when using PAM? Or is that a bit overkill?	Yes, FIDO adds security because of the hardware token that's in your pocket. As it's an offline hardware key, it is more secure than other MFA options but it's harder to manage in an organisation in case people leave, come in, lose the key, etc... It depends on your risk level.
20	Can you also go for the important cyfun label if your organisation is ISO27001 certified but not NIS2 applicable?	Yes absolutely
21	Can organisations connect to the CCB MISP to get recent IOC's?	Yes, we have a public MISP. Send your request to connect to info@ccb.belgium.be