EXAM CYBER SECURITY MANAGEMENT – APRIL 9TH 2020, 13.30 – 16.30H

Please read the instructions and integrity statement at this cover page. Please fill in the box at the end.

1. Students should follow the rules below:
   - Students are not allowed to copy-paste any piece of text from any source including their own project, study materials, the internet, etc. All answers should be written in student's own words.
   - Students **are not allowed to collaborate with each other in any way during the exam**. If there is any indication that two or more students have similar answers or that they have collaborated in any way on the exam, appropriate measures will be taken as mentioned below.
2. When taking part in an exam, students agree to comply with the rules above. In order to ensure that these rules are followed, the following measures will be enforced:
   - Today's extraordinary conditions demand extraordinary measures. Offering remote testing is one of them to ensure you – the students – can continue your learning activities. Remote testing requires taking responsibilities: if you decide to take the remote test, we count on **your honesty and integrity for 100%.** By taking this responsibility now, you and your fellow students can later show you deserve your diploma. Therefore, it is in your interest to understand that there will be zero tolerance for fraud. Accordingly, strict measures will be taken by the examination board in case students misuse our trust and commit fraud.
   - For the sake of establishing test quality, some students will be invited – after the test – to elaborate on their answers.
   - In case the teacher suspects fraud, (i) a student is obliged to take an oral exam to check whether the understanding of the student is in line with the content of the submitted test and (ii) the Examination Board will be informed. If fraud is proven, the Examination Board will take grave measures and may decide to exclude a student from participation in all module components and/ or tests for the rest of this academic year.

Good luck with your exam!

Statement of integrity

Please read the following paragraph carefully, and tick the box to acknowledge that you have done so.

By testing you remotely, we express our trust that you will adhere to the ethical standard of behavior expected of you. This means that we trust you to answer the questions in this test to the best of your own ability, without seeking or accepting the help of any source that is not explicitly allowed by the conditions of this test. Please fill in the box below the word "Agree" to mention that you agree with this statement.

RE-SIT EXAM CSM

- This exam contains 16 questions for a total of 71 points.
- The case description at the beginning of the exam applies to multiple questions.
- The exam is **open book**. Students are allowed to have access to the presentations and the reading materials in Canvas.
- Be sure to check completeness of your answers.
- **In case of questions: please call Maya Daneva at 06 14 03 66 70**
- Provide a logical and concise reasoning when asked for "why".
- Good luck!

Case description

Neon is one of the largest energy companies in the Netherlands, responsible for generating and distributing electricity, natural gas, cold & heat to its customers. Neon has to report to the Dutch Critical Infrastructure Committee (CIC) which oversees the secure and guaranteed operation of nation-wide critical infrastructure.

Neon owns multiple solar, wind & water parks, generating renewably energy. This energy is directly distributed through Neon's smart power grid, providing the required energy to its clients.

Each site, whether it provides energy, distributes or covers district heating, is managed by 2 system administrators. These administrators are fully up-to-date on the soft- and hardware used on that site.

Personnel is required to wear RFID badges to gain access to any of the buildings and wear these visibly. All personnel is required to additionally wear protective clothing and an appointment before they can access any of the production facilities.

Governance and Risk Management (8 points)

1. Neon has asked an external company to perform a penetration test against their online web portal. The report is handed over to the Security Operations Center which reviews the results and ensures the IT system owner implements the recommendations according to their priority. Neon's internal risk department reviews the results of the implementation and reports to the Dutch CIC on their conclusions.
    a. **(3 points)** Describe which stakeholders perform which role according to the three lines of defense lines of defense principle.

2. Many organizations make use of frameworks to organize their governance and risk management, as does Neon.
    a. **(2 points)** Name two advantages why Neon should use an IT Governance framework
    b. **(3 points)** Neon has decided to use the COBIT framework as their framework of choice. However, Neon has never worked with such a framework before. Do you recommend them to get a specialist on-board? Explain why you do or do not recommend them.

Industrial Control Systems (ICS) (10 points)

3. Neon has local installations of heating and cooling pumps that provide energy required for district heating/cooling. All of these types of installations consist out of multiple types of SCADA systems. Imagine you are the security specialist asked to do an assessment.
    a. **(2 points)** During your assessment, you identify that the Operational Technology (OT) systems have been connected to the IT systems. Motivate what could be the legitimate business reason to do so?
    b. **(3 points)** You are asked to validate whether the setup of the connection of OT devices to the IT environment is secure. Formulate 3 questions that you would ask and that would support you in your task.

4. Neon uses Remote Telemetry Units (RTU) to obtain information from heating radiators inside client homes to monitor the temperature and decide whether to start heating or cooling down
    a. **(3 points)** Identify three concerns that arise when thinking of this type of setup.
    b. **(2 points)** Describe a potential incident scenario if the RTU malfunctions in any way. Be sure to write the technical effects of the scenario step-by-step.

Physical and Security Awareness (8 points)

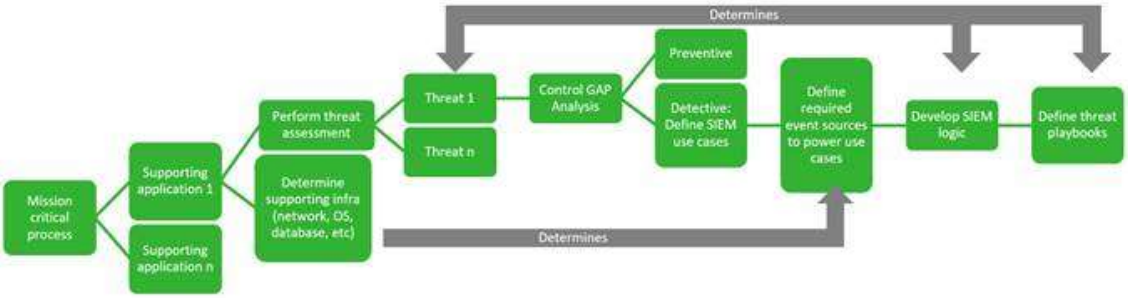
Neon is considering to perform a security assessment of their organization. They are uncertain which type is most appropriate for their situation. They have relatively limited time for execution, but are interested in a thorough security assessment report.

5. Neon is interested in red teaming, more specifically in a social engineering exercise. They would like to receive some information up front about how such an exercise works. As such, they request the attack to be performed following an attack scenario and corresponding attack techniques which is relevant to their organization.
    a. **(4 points)** How would you ensure that the chosen attack scenario reflects the attack techniques which are most relevant for Neon?

6. Trust relationships can be used during a social engineering attack.
    a. **(1 point)** Describe what a “trust-relationship” is. (from exam 2019)
    b. **(3 points)** How would you leverage a “trust-relationship” in a social engineering attack where you would try to avoid delivery costs while ordering food to get delivered.

Monitoring and Detection (12 points)

7. Threat intelligence is an important part of security monitoring.
    a. **(4 points)** Imagine that you are monitoring all your network traffic which goes to an IP-address from which your intelligence sources are stating that they are used for malicious intent. Why does this type of monitoring often generate false-positives?



8. Neon has developed a lot of internal tools which support them in managing the power grid. This source code (and thus intellectual property) is stored in a database.
    a. **(2 points)** Name two advantages of creating use cases using the process above.
    b. **(4 points)** Give an example for each of the following steps of the process above:
        i. Threat
        ii. Preventive measure
        iii. Detective measure
        iv. SIEM logic (phrase it as: *if X > 10 and not in list Y, then alert*)
    c. **(2 points)** Explain how a company might leverage the MITRE ATT&CK framework to aid in their use case design.

Identity and Access Management (IAM) (9 points)

9. Neon is looking into acquiring new Identity and Access Management tooling to harden their environment.
    a. **(3 points)** Neon has decided to use fingerprints as an authentication factor in their user authentication process. Write two factors that Neon should consider when implementing this type of control.
    b. **(3 points)** Multifactor authentication can be performed through various methods. Give 3 examples of techniques on how we use Multifactor authentication in our daily lives. (e.g. devices or techniques which allow you to authenticate).

10. Neon wants their customers to be able to access an online dashboard where they can view and manage their actual generation and usage.
    a. **(3 points)** Describe how IAM can work as an improvement in terms of user-experience for the users using the online dashboard.

Managed Security Services (12 points)

11. There is a recent publication of a critical security vulnerability in Citrix. This publication made Neon aware of the fact that they have a limited monitoring capability and feel the need to increase this capability on the short term.
    a. **(2 points)** How does outsourcing influence the growth of Neon's monitoring capabilities?
    b. **(2 points)** Write two challenges which Neon will have to overcome, if these monitoring capabilities can't be outsourced.

12. Neon has outsourced their monitoring capabilities for a while towards Netten, a Managed Security Services Provider. However, Neon whishes to renegotiate the price of the service.
    a. **(4 points)** How can Netten reduce the cost of the service, without losing quality or profit on the service contract? Identify and describe two methods.

13. Neon still thinks the new price offer from Netten is too expensive and decides to build their own monitoring capabilities.
    a. **(4 points)** What is, to your understanding, the biggest challenge Neon will face in transferring the outsourced service to an in-house capability? Motivate your answer.

Incident & Threat Management (6 points)

One of the system administrators of Neon has found signs of a potential breach. Support the system administrator in determining the impact of the breach according to the indicators. There are indicators that the attack is similar to 'Lockergoga'.

14. Neon quickly understands that they do not have the staff to investigate the incident.
    a. **(2 points)** What actions should Neon take at the least? Mention two.
    b. **(2 points)** In what sense do law enforcement agencies contribute to the incident response team?
    c. **(2 points)** What is the main reason of why investigating logs takes so much time? Motivate your answer.

Crisis Management and Business Continuity (6 points)

Neon has decided to prepare for the worst and drafted crisis management plans, so they are able to respond as effectively as possible to any unforeseen situation in the future.

15. The OODA-loop is a cycle which can serve as a framework for the crisis management organization to deal with uncertainty.
    a. **(2 points)** What is the benefit of increasing the speed in which you go through the OODA-loop?
    b. **(2 points)** What is the downside of increasing the speed in which you go through the OODA-loop?)

16. Imagine you are part of the crisis management team of Neon.
    a. **(2 points)** How would you use social media as a communication method towards your stakeholders as part of your communication strategy in times of crisis?