Cybersecurity	
Final Exam (1st Season)	
06/01/2022	**14:00 – 15:30**
Duration: 90 minutes	

Q1. (Question Value=3,0) ABCD company has been targetted with several attacks from attackers trying, and being able to, compromise their intellectual property. For this year they have planned a project to acquire and implement a security solution for the purpose of getting a better security level at their network perimeter. For that, they have sent a "Request for Quotation" (RfQ) to 3 different companies. From company 1 they got a proposal of 37,500€; from company 2, the proposal summed up to 58,500€; from company 3 they got a value of 80,000€.
You have been hired to help ABCD company to decide which will be the best solution for them, considering the following information:

- the intellectual property of ABCD has been valued as 85,000€;
- every time there's an intrusion, the company loses 75% of the asset (intellectual property) value;
- there's a 90% chance of malicious insider activity occurring in any given year;

It is asked that you justify which solution (or solutions) will be more suitable, showing all calculations, providing a proper justification for you option.
(Remark: if there's a need for any formula, you will find it after the end of the questions)

Q2. (Question Value=3,0) ABCD company wants to have a bigger and better knowledge about the vulnerabilities they have to deal with and, for that reason, they want to properly implement a risk management process.

a) Which steps do you recommend them to follow, providing a brief explanation on what to do in each step?
b) Which risk control practices would you recommend to ABCD company and why?

Q3. (Question Value=3,0). Company ABCD is now, due to the pandemic situation, putting the largest part of its workforce on remote, working from home.

a) One problem they faced is related with the need of updates on the local databases of some of the remote users, that must be able to be sure that when they download such updates from central server, they are correct and have not been changed, in purpose or accidentally. Since you have been hired as security consultant for this company, please provide the full description on how can this be achieved.

b) Another problem that ABCD is facing is concerning validation of some reports sent by remote workers to the central offices. The Administration of the company needs, also for compliance and legal questions, to ensure that those reports have been produced by certain co-workers and have not been changed after they have been sent. It is requested to you to present a solution on how can ABCD company proceed to solve this issue, presenting and justifying your answer in detail.

c) Company ABCD needs to understand how can they ensure their remote workers can have access to all applications, services, files and data in the company's computer infrastructure. For that, you are requested to explain how can this be achieved, using proper authentication mechanisms, and which recommendation you can provide to deliver the biggest possible security level.

Q4. (Question Value=3,0) ABCD company decided to create an extranet to improve the communication with business partners. They already have a firewall architecture in place, based on screened-host with a single-homed host.

a) ABCD company is requesting your advice on which could be the best firewall architecture for this purpose (and why, of course).

b) Also, ABCD company is asking you to list the factors they should consider when selecting a proper firewall for this new architecture proposed by you in a). So, list those factors.

Q5. (Question Value=2,0) ABCD company, wanting to achieve the highest possible and reasonable security level, requires, once again, you help to understand how they can improve the security on the inside of their security perimeter. They want to be sure that the firewall is not the last line of defense and that they will be able to trace and stop attacks on their internal computer network.

a) What can you propose to ABCD (tool, type,…)? Please explain.

b) Which architectures are available for implementation? Which advantages or disadvantages they present?

The End

Formulas

ALE – Annualized Loss Expectancy
ARO – Annualized Rate of Occurrence
AV – Asset Value
EF – Exposure Value
SLE - Single Loss Expectancy

SLE=AV*EF
ALE = SLE * ARO