**LEMUEL OKECHUKWU**

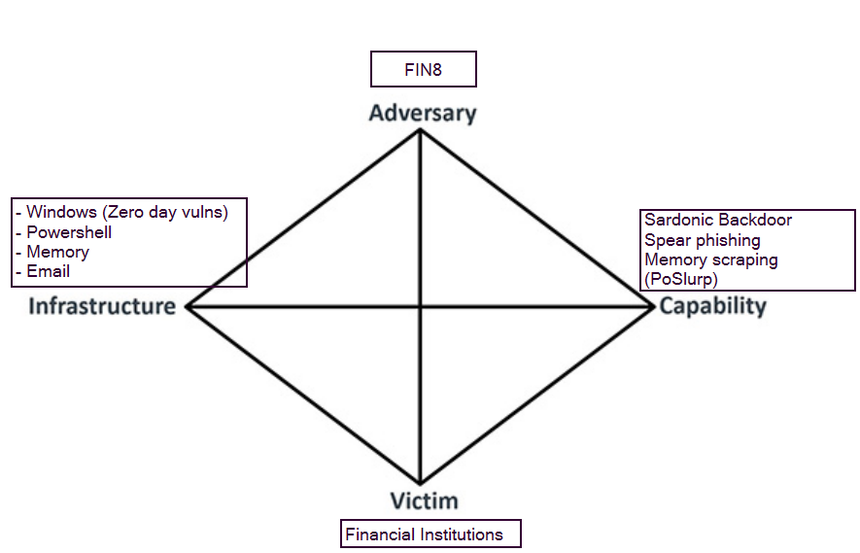
**VEPH/20B/CY082**

**TASK 35B**

**Diamond Model of Intrusion Analysis**

**TASK 35B :**

* Describe the Diamond Model of Intrusion Analysis and explain how its core components are used to analyze and correlate cyber threat activity

[](https://www.socinvestigation.com/threat-intelligence-diamond-model-of-intrusion-analysis/)

The Diamond Model of Intrusion Analysis is a framework for examining network intrusion events. It is a conceptual framework that provides a systematic approach to understanding, analyzing, and categorizing intrusions that occur within a network. It was developed by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz.

The Diamond Model is used to analyze and categorize intrusion events based on four core features:

1. **Adversary**: The entity that is responsible for the intrusion.
2. **Capability**: The tools or methods used by the adversary.
3. **Infrastructure**: The physical or digital means by which the adversary delivers the capability.
4. **Victim**: The target of the intrusion.

These four features form the vertices of a diamond, hence the name "Diamond Model". The model also includes two additional features:

* **Result**: The outcome of the intrusion.
* **Direction**: The path taken by the adversary.

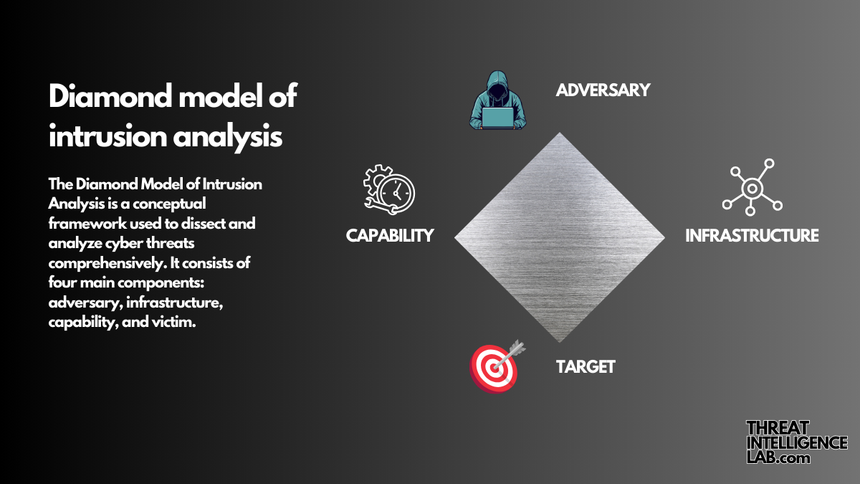
Strengths and Weaknesses

**Strengths**:

* The Diamond Model provides a structured approach to intrusion analysis, making it easier to understand complex events.
* It allows for the categorization and comparison of different intrusion events.
* It can be used to predict future intrusions based on past events.

**Weaknesses**:

* The model assumes that all intrusions can be categorized using the same four features, which may not always be the case.
* It does not account for the possibility of multiple adversaries or victims.
* It may not be suitable for analyzing intrusions that involve complex or unconventional methods.

[](https://threatintelligencelab.com/blog/diamond-model-intrusion-analysis/)

Implementation

The Diamond Model is widely implemented in the field of cybersecurity. It is used by security analysts, incident responders, and threat intelligence teams to analyze and respond to network intrusions.

Conclusion

In conclusion, the Diamond Model of Intrusion Analysis is a useful tool for understanding and analyzing network intrusions. Despite its limitations, it provides a structured approach that can help security professionals respond to intrusions more effectively. However, it should be used in conjunction with other models and frameworks to ensure a comprehensive analysis of network intrusions.