# Cyber Threat Intelligence and Incident Response Report

Cyber threat intelligence is information that is collected and evaluated by an organization to better understand the intents, capabilities, and TTPs of the malicious actors that pose threats.

Cyber threat intelligence helps reduce the risk of repeated breaches by allowing for risk mitigation strategies.

|  |  |
| --- | --- |
| Incident Name |  |
| Report Author |  |
| Report Date |  |
|  |  |

## 1. What was the indicator of attack?

|  |  |
| --- | --- |
|  |  |

## 2. What was the adversarial motivation (purpose of attack)?

|  |  |
| --- | --- |
|  |  |

## 3. What were the adversary’s actions and tactics?

Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table.

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

## 4. What are your recommended mitigation strategies?

|  |  |
| --- | --- |
|  |  |

## 5. List your third-party references.

|  |  |
| --- | --- |
|  |  |