|  | horizontal line  The Bureau Cyber Consulting  Report of:  Investigator - Your handle |
| --- | --- |
| **ㅡ** Executive Summary | horizontal line  **Purpose:** Briefly state the purpose of the report.  **Key Findings:** Summarize the major threats or incidents identified.  **Recommendations:** Highlight the key recommendations for mitigating the identified threats. |
| **ㅡ** Threat Overview | horizontal line  **Threat Landscape:** Provide a high-level overview of the current threat landscape relevant to your organization or industry.  **Threat Actors:** Describe the known or suspected threat actors involved, including their motives, capabilities, and tactics.  **Threat Trends:** Outline any emerging trends or patterns observed in the threat environment. |
| **ㅡ** Detailed Threat Analysis | horizontal line Threat Actor Profile **Name/Alias:** Name or alias of the threat actor group.  **Motivation:** Their motivations (e.g., financial gain, espionage).  **Capabilities:** Tools, techniques, and procedures (TTPs) used by the actor.  **History:** Previous attacks or incidents involving the actor. Attack Vectors **Methods of Attack:** Detail the methods used for the attack (e.g., phishing, malware).  **Vulnerabilities Exploited:** List any specific vulnerabilities exploited during the attack.  Indicators of Compromise (IoCs)  **IP Addresses:** Known malicious IP addresses.  **Domain Names:** Suspicious or malicious domain names.  **File Hashes:** Hashes of known malicious files.  **URLs:** URLs associated with the threat. |
| **ㅡ** Incident Case Studies | horizontal line  **Incident Overview:** Describe specific incidents that have occurred, including date, affected systems, and impact.  **Response Actions:** Detail the actions taken in response to the incident.  **Lessons Learned:** Summarize key takeaways from the incident |

| **ㅡ** Impact Assessment | horizontal line  **Business Impact:** Analyze the potential or actual impact on the organization’s operations and assets.  **Financial Impact:** Estimate the financial implications of the threat or incident. |
| --- | --- |
| **ㅡ** Recommendations | horizontal line  **Mitigation Strategies:** Suggest specific actions to mitigate identified threats.  **Improvement Measures:** Recommend improvements in security posture or practices.  **Training & Awareness:** Propose any necessary training or awareness programs for staff. |
| **ㅡ** Appendices | horizontal line  **Glossary:** Define any technical terms used in the report.  **References:** List any sources or references used to compile the report. |
| **ㅡ** Report Contributors | horizontal line  **Author(s):** Names and roles of individuals who prepared the report.  **Reviewers:** Names and roles of individuals who reviewed the report. |