



A HOLISTIC APPROACH TO RESILIENCE AGAINST CYBERATTACK FOR MILITARY SYSTEMS



The first step in the process of identifying and mitigating risks is to conduct a thorough risk assessment. This involves identifying all potential risks, both internal and external, and evaluating their potential impact on the organization. Once risks have been identified, the next step is to develop a risk management plan that outlines the organization's strategy for addressing these risks. This plan should include specific actions to be taken to mitigate risks, as well as a timeline for implementation.

In addition to a risk management plan, organizations should also implement a robust cybersecurity program. This program should include measures such as regular security audits, employee training, and the use of advanced security technologies. By implementing these measures, organizations can significantly reduce their vulnerability to cyber threats.

Finally, it is important for organizations to maintain a strong incident response plan. This plan should outline the steps to be taken in the event of a security breach, including how to contain the breach, investigate the cause, and notify affected parties. By having a well-defined incident response plan, organizations can minimize the damage caused by a security breach and recover more quickly.

Cyber Resilience Duria

