STUDENT ID: 45731365

STANLEY ONYEDIKA EPUNA

NIST Cybersecurity Framework methodology for Intel Corp.

Introduction:

NIST simply means National Institute of Standard and Technology. This implements specific standards aim at developing cybersecurity framework. These standards specify that the framework should have these concepts: Identify, Protect, Detect, Respond and Recover.

Intel is a technology driven company which purpose is to create world-changing technology that enriches the lives of every person on earth. So, to say, security and power efficiency is their main priority.

In 2014, A security group was formed by Intel to provide protection against security risks for people, businesses, and governments worldwide. During this course, a cybersecurity framework was formed as part of U.S. Executive Order 13636 for prioritization of security and operational leadership. This framework was developed through the collaboration of public enabling organizations and private industry. After frequent dialogue with the National Institute of Standard and Technology, a plan was devised, that is, an internal risk and management case for the framework. A pilot project was formed to develop the used case.

The Pilot project

During the early days of the development, the Intel team planned to perform a pilot project to test the framework. Intel looked for a bigger business unit with operational cybersecurity program and a solid range of products and services to test the framework limits. Intel IT met the requirements due to its broad cybersecurity program. The pilot program was completed, and it was time for it to be deployed to expand Intel's use of the Framework.

Benefits

It helped foster internal discussion. This helps in defining the various level of risk the organisation is willing to accept which is extremely valuable in prioritizing and aligning the cybersecurity risk management of the organization.

The framework of this project improves the risk management methodology and language across the internal stakeholder of the communities.

This framework helped in mapping assessments of core items by SMEs in a large heat map which helped in enabling quicker identification of outliers and visibility issues.

The pilot project being used resulted in the development of tools which can be reused when expanding the framework use across Intel. These tools include heat map, risk-scoring worksheet, customised Tier definitions.

The framework could be tailored to businesses.

Conclusion:

The Intel framework under the NIST is till under the preliminary stage, early experiences with the framework has proved valuable. The benefit gotten from the pilot project in the office and the Enterprise environment include the harmonization of the risk assessment across the enterprise, identifying strengths and opportunities to improve the framework. Plans are being made to extend this pilot framework to other areas of the Intel business functions such as Design, Services and Manufacturing. As continuous collaboration with NIST, we hope to gain better understanding of Tiers and suitable plan to explore the various categories and subcategories.

As the Framework progresses, the cyber intelligence lifecycle would be included.