Security In The Modern World

(Quantifying The Security Of Enterprises Using AI and ML)

The substantial usage of information and communication devices, and the increasing interconnectivity among systems and organizations, is exposing organizations for security risk and vulnerabilities, including intentional threat that would be associated to sabotage and vandalism. Therefore, there is a growing interest in applying risk analysis and risk managementto eliminate security problems and protect networks.

Security Risk management is an ongoing process of identifying these risks and implementing plans to

address them and risk assessment is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation. Thus, a risk assessment framework is needed with an approach for categorizing and sharing information about the security risks of the information technology infrastructure.

* **Overview of Vulnerabilities and Security**

**Framework**

System Vulnerabilities are defined as fault or weakness that reduces and limits system ability. Assessing security risk is the initial step to evaluate and identify risks and consequences associated with vulnerabilities and provide basis for management to establish cost effective security program. A security framework provides holistic structure for risk analysis covering both terminology on risk and vulnerabilities concepts and methodology for risk and vulnerabilities analysis for safety and security. The iterative process of IT security management

* **Security Assessment Overview**

Security risk assessment is being defined as the process of evaluating security risks that is conducted identifies

the required security measures.

The assessment is conducted at the very early stages of the system development as well as when there is change to

information asset or its environment. The process includes the evaluations and analysis of all asset and processes related to the system to identifying the threat and vulnerabilities that could affect confidentiality, integrity or availability of the system, and setting required control to manage the risk [1]. Risk assessment is an essential element of risk

management and to be effective, risk assessment must be an ongoing process. Depending on the purpose and the

scope of security risk assessment it can be categorized into **three types**:

**1.** **high level** assessment that can be

applied for system at design phase to identify security risks before implementation;

**2.** **comprehensive assessment** that can be used to evaluate the security risk of particular system in department to provide recommendation for improvement;

**3.** **pre-production** assessment conducted on new information system before it’s rolled out

or after there is major functional change [10].

* **HEROES OF THE SHOW**

**1.LUCIDEUS SAFE**

AI and ML backed platform to quantify, measure and mitigate enterprise wide cyber risks in real time.

A dynamic & self evolving enterprise cyber security and risk management platform that integrates with your existing IT Infrastructure and security tools deployed within your organisation to do real time assessments and provide one number (between 0 to 5), both at a macro (enterprise wide) and a micro (asset wise) level for the leadership teams to be able to visualise, track, and enhance their cyber risk posture.

**Macro Level  
Assessment**

**|**

**\/**

Using 2500+ controls encompassed over 15+ global compliances, SAFE assesses your complete IT stack and quantifies your security posture on a scale of 0 to 5

**Micro Level  
Assessment**

**|**

**\/**

Spread across 12 technology verticals spanning from Network to End-Points, SAFE provides 360 degrees view of Technology-wise Security Posture, which can be further drilled down to an individual Asset's level.

**Key Features**



**ON SAFE SCORE** -**>** SAFE gives a real-time posture analysis against the global compliance frameworks being followed in your organization

****

**REAL TIME ASSESSMENTS ->** enables the organization to have real-time assessments on their assets (Configuration Assessment).



**HACK SIMULATION ->** virtually simulate real hacks to find out your cyber defense posture against known hacks.

****

**AUTO PATCHING ->** easily remediate vulnerability and configuration controls following a change control process.



**COMPLIANCE MANAGAMENT ->** gives a real-time posture analysis against the global compliance frameworks being followed in your organization

****

