SECONIZE

Seconize Contextual Risk Enumeration

(SCORE)

Abstract

Seconize DeRisk Centre is an automated and continuous IT risk and compliance management SaaS product that proactively identifies weaknesses in the enterprise IT infrastructure, translates into risks and prioritizes them based on the business impact so that optimal investments can be made to minimize exposure.

This document summarizes the core technology *Seconize Contextual Risk Enumeration* (SCORE). The high-level approach and different advanced AI/ML technologies used for *categorization* and *prioritization* of IT risks and translation into potential business impact is explained.

Introduction

The core value proposition of Seconize DeRisk Centre (DRC) is in identifying the different vulnerabilities in the IT infrastructure and translating them into potential risks based on the Organization's context. Further such risks are prioritized using advanced decision science algorithms using numerous factors that contributed to the likelihood of the impact.

Challenges

Seconize DeRisk Centre addresses numerous challenges with contemporary IT Risk Management solutions.

Vulnerability Management

- Lack of contextualization to the Organization.
- Lack of translation of vulnerabilities into risks

Risk Management

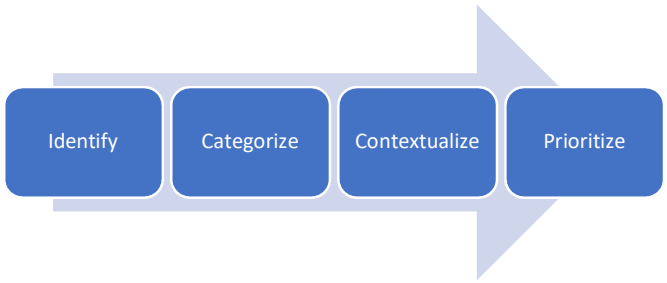
- Lack of translation of technical issues into business risks
- Lack of integration with vulnerability management processes
- Ad-hoc risk management practices using spreadsheets
- Lack of consistent and scientific approaches to prioritization of risks
- Lack of automation and near real time visibility into Organization's risk profile.

Definitions

Term	Definition	Examples
Vulnerability	A *vulnerability* is a weakness in an information system, system security procedures, internal controls, configurations or implementation of IT infrastructure.	Lack of Multifactor Authentication, Lack of Encryption, Excessive Privileges, SQL Injection
Impact	An *impact* on Organization in terms of financial, reputational losses	Loss of Productivity, Revenue Loss, Cost of investigations, Penalties, Loss of Brand Reputation
Threat	A *threat* is any circumstance or event with the potential to adversely impact organizational operations, assets, individuals through an information system.	Denial of Service, Ransomware, Phishing, Data Breach, Espionage, Outage, Theft
Threat Actor	A *threat actor* is an individual or group that can manifest a threat to the Organization.	Disgruntled Employee, Cyber Criminal, Competitor, Nation State Actor, Vendor
Risk	A *risk* is a function of the likelihood of a threat event's occurrence, by a threat actor, resulting in adverse impact	High likelihood of a cyber criminal exploiting a SQL Injection on a website resulting in Loss of Data
Risk Intelligence	A collection of information that enlists potential risks to the Organization	A prioritized list of risks identified during an assessment.
Control	A technical or non-technical information security control that remediates or mitigates a potential IT risk to the Organization	Anti-Virus, Firewall, SIEM, Information Security Policies, Security Awareness Trainings

Seconize Contextual Risk Enumeration (SCORE)

SCORE is the central technology to the contextualized risk prioritization. Its patent pending technique contains four different steps in enumerating the IT risks.



Identify

Seconize DeRisk Centre has in built powerful IT asset discovery and vulnerability scanning engine that identifies numerous weaknesses in configurations, software versions, gaps and lack of controls. A simple workflow also enables IT auditors to integrate vulnerabilities identified during manual audits. The platform is also capable of importing vulnerabilities identified by popular products like Nessus, Qualys and other scanners.

Categorize

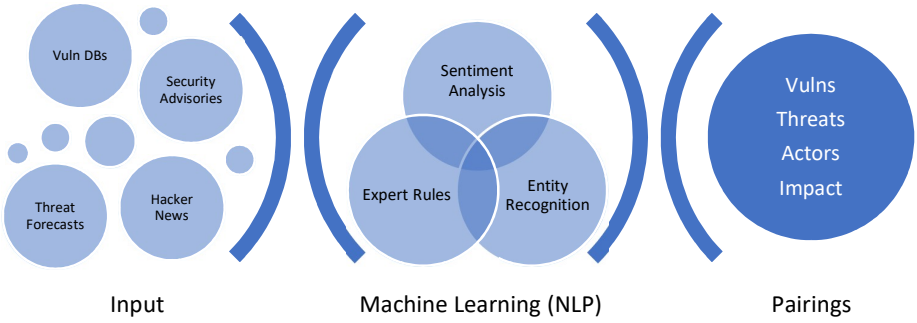
In this step, raw vulnerabilities identified are categorized appropriately by techniques that leverage both human expertise and advanced machine learning technologies.

Expert Rules

The extent of risk impact depends on the likelihood of various vulnerability and threat pairings or linkages capable of causing harm to the organisation should an adverse event occur. An exhaustive list of such vulnerability and threat mappings developed by Seconize experts leveraging from global standards and best practices is provided as input to SCORE. Further such pairings are enriched with potential threat actors, impact categories and remediation controls by experts.

Automated Classification

Seconize DeRisk Centre processes numerous vulnerability databases, security advisories, threat forecast reports using *Natural Language Processing (NLP)* techniques and automatically categorizes them into *Vulnerability-Threat* pairings identified by experts. Further such classifications are reviewed by human experts in an iterative process and false positives are weeded out. This continuous process keeps the platform abreast with evolving threat landscape.



Contextualize

In this step, the raw risk mappings identified and categorized in previous steps are personalized to the Organization. Numerous different aspects of the Organization like Industry type, Geolocation are considered. Asset attributes like reachability, type of the asset and User attributes like role are considered in personalizing the risks to that Organization.

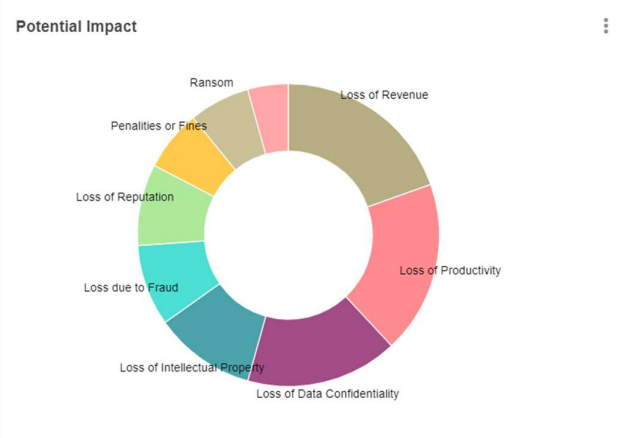
Decision Trees

Representative decision trees for the risks identified are built. Advanced decision science algorithms are applied in order determine a priority score to determine likelihood of the business impact.

Prioritize

The final and most important step in SCORE methodology is enumeration of the IT risks based on numerous risk factors and their respective attributes using the above contextualization.

Business Impact

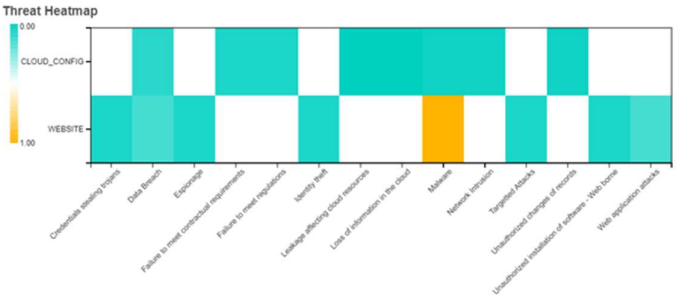


Seconize DeRisk Centre leverages SCORE technology to determine the potential impact from to the risks identified. Such impact is categorized into different direct and indirect categories.

Likelihood of losses due to loss of revenue, loss of productivity, loss of reputation and such like is projected. This crucial step helps to translate technical risks to business risks

Risk Profile

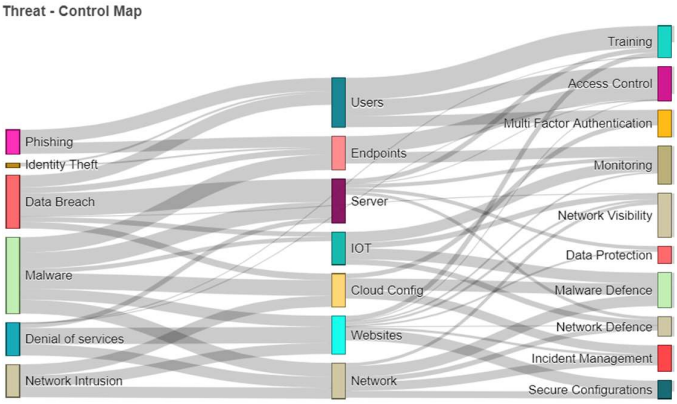
A risk profile of the entire Organization is built to give executives a big picture of the overall risk profile on a scale of 1 – 100. A detailed potential threat profile of different asset types is built.



Detailed visualizations of risk profiles based on different business units, locations and departments are also built.

Remediation

Seconize DeRisk Centre also provides the potential remediation areas to focus on.



A comprehensive threat to controls mapping dashboard provides which asset types in the IT infrastructure needs attention and suggested information security controls to be used to remediate the risks. This helps executives and IT security managers in their high level planning and prioritization of resources.

Integrations

Seconize DeRisk Centre integrates natively with existing IT infrastructure

- Integrates with IT Asset management and CMDB tools.
- Integrates with popular vulnerability management tools like Nessus, Qualys, Rapid7
- Integrates with popular threat intelligence like AlienVault, MISP and vulnerability databases.
- Integrates with incident response and ticketing systems like ServiceNow, JIRA

This helps to leverage maximum outcomes from existing investments of the Organization.

Summary

Seconize Contextual Risk Enumeration (SCORE) is a patent pending IT risk prioritization technology leveraging advanced machine learning algorithms like natural language processing for automatic translation of vulnerabilities into risks and decision science algorithms for contextualized risk prioritization and potential business impact.