RiskMate®

atamai.technology

DATA SHEET

CyberRisk Continuum™

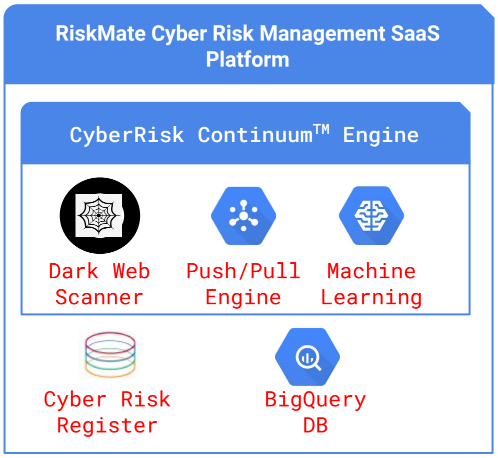
The core component of RiskMate® SaaS platform is the underlying patent pending CyberRisk Continuum™ engine. It enables monitoring through various pull and push methodologies by tracking emerging threats and vulnerabilities from dark web and other proprietary sources. The SaaS solution harnesses the power of analytics and machine learning by tracking risk postures of critical assets of similar class and/or category across the platform. When new risks are identified, asset owners are alerted to take corrective actions to mitigate potential and emerging risks.

Key Features

CyberRisk Continuum™ relies on the following capabilities provided by the engine.

➢ Industry Peer Analytics

The patent-pending feature monitors risk posture of critical assets that are grouped by asset category, asset class and asset type. When a new risk is identified for an asset by a tenant through the risk assessment process, underlying event engine detects and pushes the risk to a list of industry peer subscribers with a similar asset category, asset class or asset type. The analytics engine evaluates and assigns the risk to the assets, if applicable. The event engine notifies asset owners to accept or reject the risk. Further risk mitigating actions will be required by the asset owners if the risks are accepted.



➢ Emerging Threats and Vulnerability Scanner

Another key patent-pending method for CyberRisk Continuum™ engine relies on a dark-web scanner. It leverages proprietary sources and methods to scan for emerging threats and vulnerabilities for critical assets under monitoring. A common taxonomy mapping translates emerging threats and vulnerabilities to internal system. The analytics engine evaluates and assigns the risks to the assets as applicable. The event engine notifies asset owners to accept or reject the risk. Further risk mitigating actions will be required by the asset owner if the risks are accepted.

➢ Threats and Vulnerabilities from Known Sources

One of the core components of the CyberRisk Continuum™ is the Push and Pull Engine. This component can interface with other known sources of threats and vulnerabilities data aggregators and pull and store it in the cloud storage. The analytics engine then evaluates the risk impact and take appropriate action by creating a risk in the risk register for further action by asset owners. If a tenant has other vulnerability, threat management and proprietary systems can push asset specific risk information through the API layer to RiskMate platform for further action.

For further information please contact:
info@atamai.technology