REPORT

Setting Alerts Based on Marsh McLennan Cyber Risk Analytics Center Research Findings

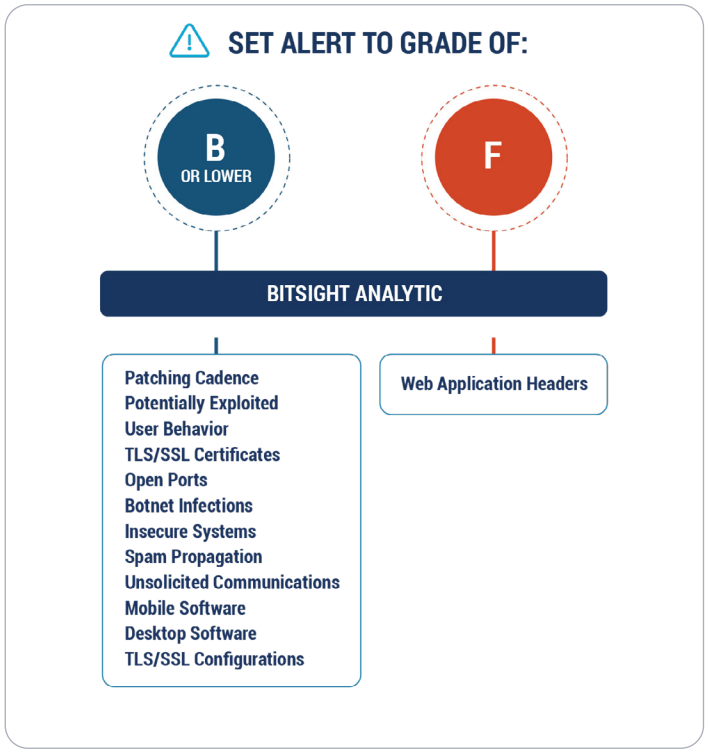
How BitSight customers can leverage this information to optimize product alerts

Marsh McLennan Cyber Risk Analytics Center conducted an independent analysis to quantify the relationship between BitSight's data analytics (Security Rating and risk vectors) and Marsh McLennan Cyber Risk Analytics Center's cybersecurity incident data. After comparing the security performance data of thousands of organizations that experienced cybersecurity incidents against those that did not, **Marsh McLennan Cyber Risk Analytics Center identified 14 BitSight analytics to be statistically significant and correlated with cybersecurity incidents, including the BitSight Security Rating and 13 key risk vectors.**

BitSight customers may wish to leverage these research findings to optimize their alert settings within the BitSight platform. Setting alerts is a critical part of managing your own cybersecurity performance and the cybersecurity performance of your third-party vendors.

For those users interested in incorporating Marsh McLennan Cyber Risk Analytics Center's research findings into their security strategy, BitSight has reported below the grades/ratings thresholds that may be of particular concern to BitSight customers. According to Marsh McLennan analysis, each risk vector grade below corresponds to the grade at which an organization is at an increased likelihood, of at least two times, of experiencing a cybersecurity incident relative to high-performing peers.

Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022



Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Please read the full report to learn more about the findings.