SecurityScorecard

Scorecard Event Log™

Gain transparent visibility into all score changes

Scorecard Event Log introduces transparency around score changes by showing a clear historical record of all fluctuations in a scorecard, plus any security-related events, that have impacted an enterprise or vendor score. This new functionality enables customers to view and fully understand which issues caused scores to change over time.

Capabilities

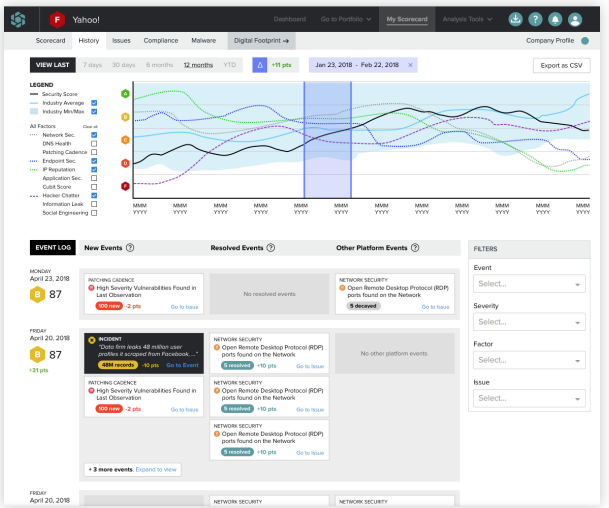
Use Scorecard Event Log to:

- Identify issue changes that have had a positive or negative effect on factor score and overall grade changes beginning September 4th, 2018*
- Search through a clear record of all fluctuations in a scorecard
- Discover specific changes between two points in time, including which issues impacted the overall grade and to what degree
- Create audit reports with exported CSV data that list resolved issues and the impact that these remediations had on scores

* Scorecard Event Log shows issue changes leveraging Next-Gen Scoring, the new scoring methodology, effective September 4th, 2018. Scorecard Event Log cannot display issue-level data prior to September 4th since it would require use of the legacy methodology. However, factor-level and overall grade change data will continue to display in the History chart for all dates.

Continuously Monitor the Security Health of Any Organization

SecurityScorecard provides instant visibility into enterprise security posture as well as the cyberhealth of all vendors and partners in any organization's ecosystem. The platform uses trusted commercial and open-source threat feeds, and nonintrusive data collection methods, to quantitatively evaluate and continuously monitor the security posture of thousands of organizations worldwide. SecurityScorecard delivers the most accurate, transparent, and comprehensive security risk ratings available for small to large enterprises in every industry sector.



Sample view of Scorecard Event Log. Actual platform interface may contain slight variations.

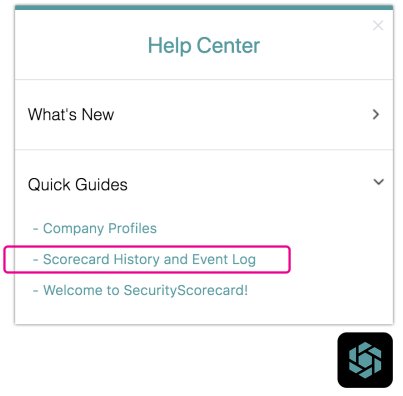
Sample Use Cases

Use Case 1: Governance, Risk, and Compliance

Activate and monitor event-level audit logs to ensure continuous detection of cyber activity and integrity of key data elements. Event-level chronological data enables the review, examination, and reconstruction of system and data processing. These activities are key components of your ongoing efforts to maintain compliance with GRC regulatory frameworks and standards.

Use Case 2: Internal Auditing

If a vendor or enterprise score drops from A to B, for example, you can quickly render a log of all issues that appeared and were resolved during a specific date range, while also evaluating each issue's severity and score impact. In addition, on the Findings page, you can track how individual issues were resolved, using compensating controls, refutes, or other means.



Get Started

Visit the History tab in any scorecard to start using this new feature. Find user information in the Quick Guides section of the Help Center, including "Scorecard History and Event Log," a walk-through of your own Scorecard Event Log.

Try the new Scorecard Event Log today. Get a whole new perspective of score fluctuations and a comprehensive log of issue changes – critical information that supports adherence to relevant regulatory compliance requirements.

Digicy Cloud
Joram Teusink
+31850290572
joram@digicy.cloud
www.digicy.cloud