Cyber Posture Rating Explained

GIORA OMER, CHIEF ARCHITECT, PANORAYS

Introduction
The Panorays platform assesses companies and generates a rating that reflects the company’s cyber posture. This rating, together with other factors like the security questionnaire, is used by Panorays’ customers to make security decisions regarding their third parties.
Panorays performs a non-intrusive assessment of the third party’s external digital footprint. Since the assessment is not invasive, it can be performed continuously and without the consent of the assessed party. This means that the assessment data is collected from:

- Open source intelligence (e.g. asset reputation feeds)
- Public domain data
- Light probes (e.g. proprietary collectors similar to search engine indexing bots)
- Various APIs and data feeds

Panorays is a 100% SaaS-based platform. The Panorays assessment is performed externally and does not have access to internal company resources. That said, some of the public sources include feeds, such as botnet activity, which allow for a deeper internal look of the company without the need to be intrusive. Many Panorays findings provide specific vulnerability information, e.g. by technology version, CVE correlation or from bug bounty programs. However, Panorays does not perform active penetration tests such as running exploits or brute forcing.

Probing company services, including but not limited to web servers, mail servers, DNS, SNMP, SSH and NTP, can reveal security configurations and practices performed by the company. The external digital presence and exposure says a lot about the security hygiene of a company. The amount of data that can be obtained about any company in this manner is staggering. Using big data analytics and experienced research capabilities, the Panorays platform delivers a thorough look into the assessed company’s security gaps (also called findings). Accordingly, the platform generates a rating which reflects the cyber posture of the assessed company.
**Continuous Monitoring**

Panorays continuously performs the reconnaissance phase and monitors the assessed company so that the platform alerts of critical new findings or significant changes to the Cyber Posture Rating. This is unlike different assessment methodologies like penetration tests and questionnaires that become outdated immediately once they’re completed.

**Asset Discovery**

The Panorays platform identifies a large percentage of the company’s attack surface through its Asset Discovery Mechanism. This mechanism enables Panorays to generate a very low affiliation false positive rate.
Ratings Methodology

The basis of the Panorays ratings methodology is the Test entity. Each assessment comprises 100+ Tests that are run on the discovered company assets (servers, DNS, IP ranges, etc.). All of the tests are prioritized with various severity levels.

The results of each Test generates findings and a rating, and the aggregate of all ratings generates the final rating of the company.

Some Test examples:
- Do the company mail servers have an SPF record?
- Do the company web servers support deprecated SSL protocols?
- Are company assets flagged as hosting malicious activities?

The Tests are divided into three sections: Network and IT, Application and Human.
**Test Rating Calculations**

Each Test has its own internal 0–100 rating, which is rated as follows:

**100:**
The Test was performed but no findings were detected (all assets passed the Test).

**0:**
The Test was performed and all assets failed the Tests (findings count = assets count).

**N/A:**
The Test could not be performed (e.g. no SNMP server was detected so the SNMP Test could not be run).

**1–99:**
Some assets passed the Test while others failed.

The Tests have different rating calculation functions, to provide the most precise results for each Test. Different calibration parameters are as follows:

- **Simple relativity.** For example, if two out of 10 assets have a finding, the Test rating will be 80.

- **Statistics.** For example, if one out of 100 assets has an open database, Panorays won't rate the Test as 99.

- **Company and industry standards.** For example, a company with 20 employees should not have the same security team size as a company with 20,000 employees.
The Development of Tests

Tests are based on two security aspects:
1. Industry best practices like OWASP and NIST
2. Research know-how (proprietary knowledge)

Together, Panorays generates a roadmap of Tests and categories to be added to the assessment engine.

Each Test is examined for prioritization and considers questions such as the following:
• What can the Test tell us about the cyber posture of the company?
• What is the Test severity?
• Can the Test be performed in a non-intrusive manner?

In particular, the Data Collection and Tuning phases are crucial. Every Test is initially deployed in hidden mode to collect data from at least tens of thousands of companies in the Panorays database. The data is then used to corroborate the researcher’s know-how and tune the severity and weight of the Test.
Test Categories

The Tests are divided into three top-level sections: **Network and IT, Application and Human**.

The rating for each category is an aggregate of all Tests run under that category. The category ratings help the user focus on problematic areas in the assessment and compare between companies based on the categories.

**Note:** The final rating is not derived from the category ratings, but directly from the Test ratings. This is done in order to increase the accuracy of the Test’s impact, such as N/A Test results, critical findings, etc.
**Assessment Release Management**

The list of Tests, severities, and weights is called an Assessment Template. There is a single enabled Assessment Template at any given time. Because changing the template may affect the Cyber Posture Rating, each change in the template (adding tests, changing weights, etc.) is documented and monitored.

**Challenging False Positives**

Panorays allows third parties to easily dispute findings and assets as follows:
1. The supplier is invited to the Panorays platform to review findings and assets.
2. If the supplier feels that any of the data is inaccurate, he or she simply clicks "claim dispute," adds any comments about the finding or asset, and submits.
3. Panorays validates the data internally within 24 hours, accepts or rejects the claim and updates the findings accordingly.
4. The supplier’s Cyber Posture Rating is automatically updated according to the new external footprint assessment.

<table>
<thead>
<tr>
<th>Accuracy rate</th>
<th>False positive rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>99.4%</td>
<td>0.6%</td>
</tr>
</tbody>
</table>
Summary

The Panorays Cyber Posture Rating delivers:

1. **Accuracy.** The ratings consist of numerous Tests that are checked against a large dataset for distribution and a trusted dataset for validation. Ratings consider different aspects of companies like size and industry. Breached companies are systematically investigated to check that the ratings could give the appropriate indication for the breach.

2. **Transparency.** All of the Tests performed by the assessment engine are displayed with their results. Both the evaluator and the mitigator (supplier or third-party) can view the entire findings list and discovered assets that build the rating—and dispute any of the findings, if necessary.

3. **Consistency.** The same Tests are performed for all companies. The rating is absolute.

4. **Stability.** A company’s Cyber Posture does not change that often. The rating is typically built from hundreds of Tests on thousands of assets. The rating should provide an indication of the general cyber posture of the company and not of a specific finding, critical as it may be. The contextual data indicating business impact and temporal factors (e.g. critical findings) are emphasized in the Risk Rating to make the Cyber Posture Rating as stable as possible.
FAQ

Does Panorays assess internal (intranet) assets?
The Panorays assessment is performed externally, and does not have access to internal company resources. However, there are findings taken from public sources that are generated by internal resources, such as botnet activity.

Does Panorays run active tests on company assets?
Panorays does not perform active penetration tests like running exploits or brute forcing. However, many findings provide specific vulnerability information (e.g. by technology version, CVE correlation or from bug bounty programs).

How does the Panorays assessment compare to a penetration test?
This is like comparing apples to oranges, but here are the major differences:
1. Penetration tests are active and intrusive. They require consent and coordination with the assessed party, as they can cause disruption of services. The results of a pentest may be more precise, as each exploit can be verified and tests can be run on internal assets as well.
2. Panorays assessments are generally more comprehensive, as they include all of the company’s publicly-facing assets, also known as the external attack surface. The Panorays assessment engine can identify changes in the attack surface, such as added assets, and update the ratings and findings accordingly.
3. Panorays assessments are continuous. A pentest may be invalid a day after it is performed; for example, if a new vulnerability comes out. Panorays continuously updates its vulnerability database and can notify when new critical findings are detected or if there is a significant change to the Cyber Posture Rating.
4. Panorays is 100% SaaS-based, no installation required. Various automated pen-testing tools require an agent, and hence the installation and maintenance from the side of the third party.

How does the Panorays assessment compare to a vulnerability scanner?
A vulnerability scanner typically is a Web-based test on predefined assets. Additionally, the scanner runs intrusive scans that require consent from the third party. Panorays widens the checks and it’s not scoped; rather, it performs the reconnaissance phase continuously.
Panorays automates third-party security lifecycle management. It is the only platform that provides organizations with a rapid thumbs-up-or-down view of supplier cyber risk by inherently combining automated dynamic security questionnaires with external attack surface evaluations and business context.

Companies using Panorays dramatically speed up their third-party security evaluation process, streamline transparent collaboration between teams and suppliers, eliminate manual questionnaires, gain continuous visibility and ensure compliance to regulations like GDPR and NYDFS.

Panorays is a SaaS-based platform, with no installation needed, and integrates into existing organizational workflows. It is trusted by global organizations in industries including financial, insurance, healthcare and technology.