Panorays

Cyber Posture Rating Explained

Introduction

Given the precipitous rise in ransomware and data breaches, it's important for organizations to mitigate their own cyber risk and also bring the security of their third parties into alignment with their security controls, regulations and risk appetite. To help do that, Panorays non-intrusively evaluates your own company's and your third parties' attack surface by performing hundreds of tests, such as collecting information on exposed assets or checking a lack of security best practices. Once the analysis is completed, typically within hours, each company assessed receives a Cyber Posture Rating from 0–100, representing the risk level attributed to its external digital perimeter. To help you manage the security risk related to your third parties, Panorays combines this rating with the results of the third party's Smart Questionnaire™ and the business context of your relationship, providing you with a rapid, accurate view of supplier cyber risk.

01

External Attack Surface Assessment

Overview

Panorays evaluates each company's attack surface in a non-intrusive manner, through the analysis of externally available data. To ensure a comprehensive view of an organization's digital perimeter, Panorays performs hundreds of tests to assess three different layers:

01

Network & IT

Web, e-mail and DNS servers, TLS protocols, asset reputation, cloud solutions and other exposed services.

02

Application

Web applications, CMS, domain attacks, etc.

03

Human

Employees' attack surface, social posture, presence of a dedicated security team, etc.

Example findings within the Network, IT and Application layers could include untrusted TLS certificates, a missing WAF on a significant asset, exposure of WordPress user data, an unpatched application version, etc. In addition, Panorays considers the effect of human behavior in a company's external attack surface assessment—and is the only platform that does so. Example findings here could include high employee attack likelihood based on social media presence, lack of employee security awareness or the absence of a dedicated security team.

Asset Discovery Mechanism

Taking one step back, before we can start performing the external assessment tests, we need to identify every publicly accessible asset linked to the evaluated company. Asset discovery is done automatically by the Panorays platform, requiring only a single asset to get started. Usually, the primary domain of a company is used as a starting point for discovering all of the company's attack surface, including domains, subdomains and IP addresses.

Continuous Monitoring

While the initial assessment is typically completed within hours, Panorays continuously updates the Cyber Posture Rating based on changes to the company's external footprint. That's because a point-in-time view doesn't keep up with the evolving risk landscape, as risk can change by the second. Security teams receive live alerts about any security changes or breaches to their company or third parties.

Non-Intrusive Assessment

As the assessment is external and not intrusive, it is performed by Panorays without engaging with the assessed company itself. That being said, you and your third parties can easily dispute irrelevant assets or findings through the platform. This external mechanism enables quick results, typically within hours, while maintaining an extremely high accuracy rate.

Assessment data is collected from both public sources, such as asset reputation feeds, and common probes, such as sending an empty email to see whether a destination actually exists. As for the amount and level of information obtained using an external assessment, the results are staggering:

- 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.
- 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.
- Panorays provides specific vulnerability information; for example, by technology version, CVE correlation or from bug bounty programs.

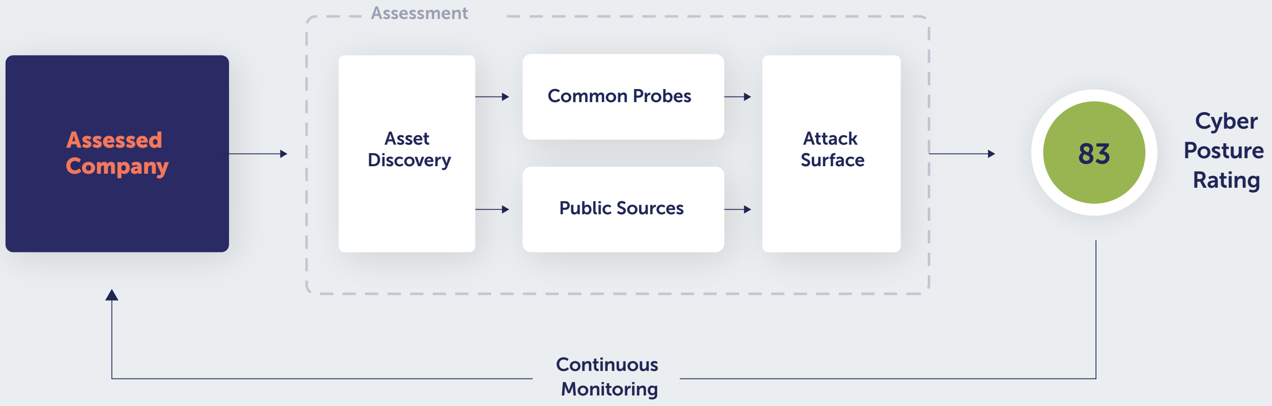


Figure 1: How Panorays assesses companies' attack surface

02

Cyber Posture Rating Methodology

Overview

The basis of the Panorays Cyber Posture Rating methodology is the Test entity. Each assessment consists of hundreds of Tests that are run on the discovered company assets (servers, DNS, IP ranges, employees, etc.).

The results of each Test generate findings (e.g. cyber gaps) and a Test rating. The aggregation of all Test ratings generates the final Cyber Posture 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?**

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.

Each Test has different rating calculation functions, to ensure the most accurate results. The 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.

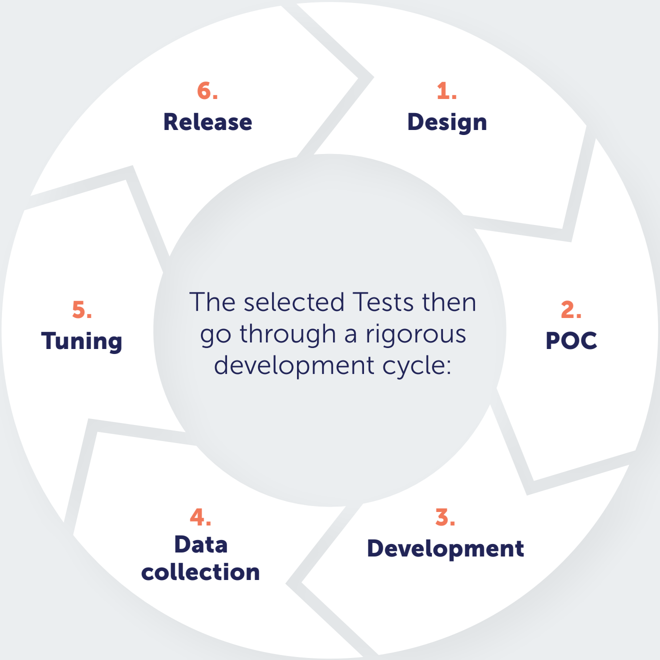
Company and industry standards. For example, a company with 20 employees should not have the same security team size as a company with 20,000 employees.

The Development of Tests

Panorays develops Tests based on both industry best practices, such as OWASP and NIST, and the cybersecurity knowhow of our team of research experts. The team continually adds new Tests based on changes to the threat landscape and Panorays' extensive experience in this domain.

The team answers the following questions for each Test under review, in order to decide whether to add it to the assessment engine:

- **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?**



The selected Tests then go through a rigorous development cycle:

In particular, the Data Collection and Tuning phases are crucial. Every Test is initially deployed in hidden mode to collect data from the 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.

For example, Panorays researchers initially set a baseline of medium severity and weight for the existence of DNSSEC. After running the Test on all companies in the Panorays database, the researchers obtained the following information:

- 97% of companies don't have DNSSEC at all
- The average test rating is 1.7 points out of 100
- A trusted companies dataset (Google, Amazon, Microsoft, etc.) has an average rating of 1.6 points

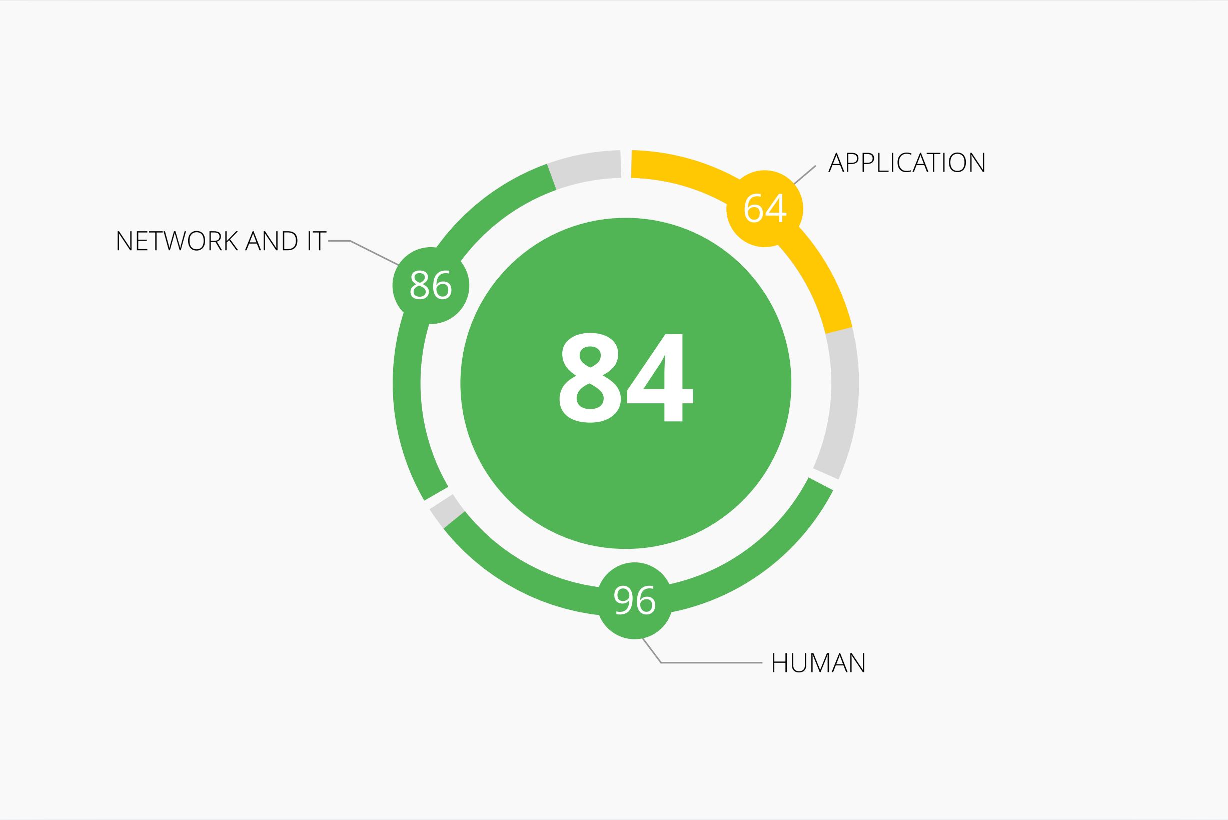
The results indicated that DNSSEC is not widely adopted; therefore, the Test weight should be tuned appropriately. The results are verified and approved by the researcher before finally being added to the assessment.

Test Categories

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

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

Accuracy rate	False positive rate
99.4%	0.6%

Summary

The Panorays Cyber Posture Rating delivers:

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.

Transparency

All of the Tests performed by the assessment engine are displayed with their results. All parties can view the entire findings list and discovered assets that build the rating—and dispute any of the findings, if necessary.

Consistency

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

Stability

A company's Cyber Posture Rating is typically built from hundreds of Tests on thousands of assets. The rating provides an indication of the general cyber posture of the company and not of a specific finding.

FAQ

01 Does Panorays assess internal company assets as part of the external attack surface assessment?

As the assessment is external and not intrusive, it is performed by Panorays without engaging with the assessed company itself. This means we do not have access to internal company resources. The amount and level of information obtained using an external assessment is remarkable, allowing Panorays to perform comprehensive, accurate assessments at scale, without the hassle of intrusive assessments requiring agents' installation.

02 Does Panorays run active penetration tests on the assessed company assets?

As the Panorays assessment is completely external, it does not perform active penetration tests such as running exploits or brute forcing. This does not prevent Panorays from identifying vulnerabilities related to the company assets. Many findings from Panorays' non-intrusive tests provide specific vulnerability information (e.g. by technology version, CVE correlation or from bug bounty programs).

03 What are the key benefits of Panorays' non-intrusive assessment compared to a penetration test?

Speed and Scalability

Penetration tests are active and intrusive. They require consent and coordination with the assessed party, as they can cause disruption of services. Automated pentesting tools require an agent, and hence the installation and maintenance from the side of the third party.

Panorays is a SaaS-based platform, requiring no installation on the customer or third-party side. Panorays' external assessment requires minimal effort from the assessing company — simply adding the assessed company name and domain. The assessment is typically completed within a few hours, enabling organizations to perform assessments at scale.

Breadth

Panorays' assessments are generally more comprehensive than penetration tests, 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.

Continuous View

A pentest will be invalid a day after it is performed; for example, if a new vulnerability comes out. Panorays' assessment is continuous, alerting security teams about any security changes or breaches to their third parties.

04 How does the Panorays assessment compare to a vulnerability scanner?

Vulnerability scanners are web-based tests on pre-defined assets. They run intrusive scans that require consent from the third party. Panorays' assessments are much more comprehensive, and do not require consent.

Want to learn more about how Panorays can help with your third-party security process? Contact your Panorays sales rep or email us at info@panorays.com

About Panorays

Panorays quickly and easily automates third-party security risk evaluation and management — handling the whole process from inherent to residual risk, remediation and ongoing monitoring. Unlike other solution providers, Panorays combines automated, dynamic security questionnaires with external attack surface assessments and business context to provide organizations with a rapid, accurate view of supplier cyber risk. It is the only such platform that automates, accelerates and scales customers' third-party security evaluation and management process, enabling easy collaboration and communication between companies and suppliers, resulting in efficient and effective risk remediation in alignment with a company's security policies and risk appetite.

The company is offered as a SaaS-based platform and serves enterprise and mid-market customers primarily in North America, the UK and the EU. It has been adopted by leading banking, insurance, financial services and healthcare organizations, among others. Headquartered in New York and Israel, with offices around the world, Panorays is funded by numerous international investors, including Aleph VC, Oak HC/FT, Greenfield Partners, BlueRed Partners (Singapore), StepStone Group, Moneta VC, Imperva Co-Founder Amichai Shulman and former CEO of Palo Alto Networks Lane Bess.

Visit us at www.panorays.com