T

Threat Landscape: Meaning and How to Assess Your Risk

A threat landscape describes the threats relevant to a particular environment and period: actors, methods, targets, exploited weaknesses, and potential consequences. Use it to prioritize security work by comparing external observations with your own systems and exposure. A global trend is context, not proof that your organiza...

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What belongs in a threat landscape?

02 Threat landscape vs. attack surface and threat intelligence

03 How to read a threat report critically

04 A practical assessment workflow

05 Example: turning an advisory into an action

06 How often should it be updated?

Quick answer: A threat landscape describes the threats relevant to a particular environment and period: actors, methods, targets, exploited weaknesses, and potential consequences. Use it to prioritize security work by comparing external observations with your own systems and exposure. A global trend is context, not proof that your organization faces the same likelihood or impact.

01 What belongs in a threat landscape?

A useful landscape states its scope. It might cover a country, industry, technology, or individual organization over a defined period. It connects reported activity to the systems and services that could be affected. Without that context, a list of attack names provides little help in deciding what to fix first.

- **Actors and objectives:** who may cause harm and what they seek.
- **Methods:** observed intrusion, fraud, disruption, and persistence techniques.
- **Targets:** relevant devices, accounts, applications, suppliers, and data.
- **Exposure:** weaknesses and reachable services that make an attack plausible.
- **Consequences:** interruption, financial loss, disclosure, or other effects.
- **Evidence and uncertainty:** sources, dates, coverage, and confidence in the assessment.

02 Threat landscape vs. attack surface and threat intelligence

Your attack surface consists of the systems, interfaces, identities, and other opportunities through which an adversary could interact with the environment. The threat landscape describes the threats around that environment. Threat intelligence evaluates information about threats to support decisions. A risk assessment brings those observations together with likelihood, impact, and existing controls.

These activities inform each other. Discovering an exposed administrative service can make a previously low-priority advisory immediately relevant. A report about a technology you do not use may require no direct action after its applicability is checked.

03 How to read a threat report critically

Check the observation period, geography, sector, and population before using a statistic. A vendor's detections among its customers are not a census of all attacks. Reported incidents also reflect reporting practices and visibility. A rise in detections may follow better monitoring rather than a matching rise in successful compromise. For example, a report about increased phishing should prompt a review of your own email and account exposure, rather than an assumption that every team faces the same risk.

Separate counts from rates and attempted activity from confirmed incidents. Look for a consistent denominator before comparing percentages across reports. Preserve the original source and date so a future reviewer can understand why a decision was made.

04 A practical assessment workflow

1. Define the business decision, such as which exposed services need urgent remediation.
2. Inventory relevant assets, identities, supplier connections, and important dependencies.
3. Collect applicable vendor advisories, government guidance, sector reports, and internal incident evidence.
4. Check whether the affected versions and attack paths exist in your environment.
5. Assess business consequences and the controls already in place.
6. Assign an action, owner, deadline, and method for verifying completion.
7. Record uncertainty and revisit the assessment when evidence or exposure changes.

05 Example: turning an advisory into an action

Suppose a report describes exploitation of a remote-access product. First confirm whether your organization uses it, which version is installed, and whether the vulnerable function is reachable. Then check the vendor's remediation and any relevant internal evidence. The result might be a software patch, temporary access restriction, or investigation—not simply forwarding the headline to everyone.

A useful action record names the affected service, the evidence, the responsible owner, and what success looks like. For example, verify the installed fixed version and the removal of unnecessary public exposure. This makes the assessment auditable and keeps trend monitoring connected to practical work.

06 How often should it be updated?

Choose a regular review cadence that fits the organization, and also update after significant incidents, major exposure changes, or urgent advisories. Keep dated snapshots when reporting trends. An evergreen glossary explains the method; a current threat assessment should state the actual period and sources rather than silently reusing last year's conclusions.

References: ENISA's threat landscape methodology and NIST threat assessment terminology.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com