CYCOGNITO

TECHNICAL DATASHEET

Prioritization and Remediation

Confidently resolve issues on your external attack surface

Today's security teams often prioritize issues using legacy CVSS scores, spreadsheets, and personal opinions.

Even CVSS v3, which introduces two additional layers of severity (none and critical), lacks the business context and security test information required to understand the risk to your business and confidently assign remediation resources.

Business exposure, not the number of CVEs, should drive prioritization efforts.

Prioritizing exposures is one of the most important and difficult areas of cybersecurity security today. With thousands of risks to monitor, classify, and remediate, and new CVEs added every 18 minutes on average[1], it's difficult for teams to focus their efforts on the most meaningful problems. With CyCognito, you will:

Remediate confidently and efficiently

Help your teams work at their highest efficiency with the knowledge of asset location, business context, security test data, and detailed remediation steps. With CyCognito, confidently address the 2% of your issues that cause 95% of risk.

Reduce false positives with issue validation

Reactive security workflows leave assets exposed and force your teams to play catchup, increasing mean time to remediation (MTTR). With CyCognito, each issue is validated automatically to ensure low false positives.

Access risk-based context that matters

Unique CyCognito context *asset attractiveness and asset discoverability* tie business and security information to enable confident risk-based decisions.

Reduce time-consuming manual research

Typical remediation efforts require manual research to determine where the asset resides and how to fix the exposure. CyCognito eliminates wasted time by providing remediation instructions, attribution information, and an estimate of effort.

Validate remediation efforts automatically

CyCognito's active testing validates remediation efforts, eliminating the need for manual review and avoiding a false sense of security on assumed remediation success.

Develop remediation plans based on business goals

Create an actionable plan for improving your organization's security posture with a prioritized list of assets, issues and the effort needed to address them.

1. NIST shows 28,830 CVEs released in 2023, divided by 525,600 minutes in a year, equates to 1 CVE every 18.2 minutes

How CyCognito Issue Prioritization Works

Risk-based prioritization is only possible with a complete asset inventory, accurate business context and high-confidence security test results. CyCognito's automated prioritization pipeline consistently discovers, tests, and prioritizes exposures across your external attack surface.

CYCOGNITO PRIORITIZATION PIPELINE

01

External Asset Inventory

Integration with our discovery engine[2] ensures that our prioritization engine has the most up-to-date external asset inventory.

02

Asset Business Context

Extensive business context is added for deep insight into your organization's use of the asset and business criticality. Examples:

- Organizational business structure discovery identifies where the asset exists in your organization across geography/subsidiary/brand/etc.
- Certainty scores tied to all ownership information, with evidence
- Running services, open ports, environment data, etc. provide visibility into asset use within the organization

03

Security Test Results

Highly accurate active security testing is performed on all assets[3] including dynamic application security testing (DAST) for web apps, data exposure tests, compliance violation tests and more. Examples:

- Issue type, category and business impact
- Exploitation complexity and method
- Detection complexity and potential impact
- Remediation effort

04

Threat Intelligence

Exposures and vulnerabilities are compared to third-party sources such as CISA Known Exploited Vulnerabilities (KEV) and dark web threat intelligence to provide real-time insight into exploit weaponization and cybercriminal behavior. This information is reflected in the final score.

05

Risk Context

Unique CyCognito risk context are calculated and assigned to each asset.

- **Asset Discoverability** - How easily an attacker can find the asset and identify its relation to your organization
- **Asset Attractiveness** - How attractive an asset may be to an attacker based on running services, exposure, business context and more.

06

Scores and Grades

Asset and issue context are used to build a score using CyCognito's proprietary enhanced severity scoring engine. These scores, and the resultant grade, provide your most accurate visibility into external risk.

2. CyCognito Discovery & Contextualization technical datasheet: https://www.cycognito.com/resources/datasheets/discovery-and-contextualization/
3. CyCognito Active Security Testing technical datasheet: https://www.cycognito.com/resources/datasheets/active-security-testing/

Understanding CyCognito Risk-Based Scoring

Security scoring and grading are crucial for prioritizing your remediation efforts. Risk-based scoring ties the criticality of the asset to your organization with high-precision active security test results and provides the most accurate assessment of risk.

Asset Attractiveness and Discoverability

Not all assets are equal in the eyes of attackers. The concept of attractiveness plays a pivotal role in determining an asset's risk profile. CyCognito's asset attractiveness context includes the concept that the asset is valuable, discoverable, and easy to exploit. Combined, discoverability and attractiveness form the basis for assessing which assets represent the greatest risk to your organization.

For example, consider two assets with an identical number of severe issues. While they might initially appear to have the same risk level, their attractiveness to an attacker can significantly differentiate their risk. An asset using RDP might be more appealing to attackers due to its location in the network and ability to gain rapid access. Another asset with similar issues but less strategic importance might pose a lower risk.

What CyCognito Scores and Grades Mean

CyCognito's security score, on a scale from 0 to 100, offers granular insight into an asset's security status, while the security grade, ranging from A to F, categorizes assets into broader risk segments.

Grade	Score	Description
A	100	**No risk** – CyCognito has not found issues on these assets.
A	90–99	**Very low risk** – There are either no issues or only low severity issues on these assets. There is little to no value in spending effort on these assets' issues.
B	70–89	**Low risk** – A few assets in this group may have a low probability of exploitation, but even if exploited the implications are limited.
C	40–69	**Medium risk** – A moderate amount of assets in this group may have medium-severity issues. Issues that have a good probability of exploitation may have limited implications. However, those that have a low probability of exploitation may have severe implications.
D	15–39	**High risk** – A sizable amount of assets in this group may have high-severity issues, which have a high probability of exploitation at some point, with possibly severe implications.
F	0–14	**Critical, immediate risk** – A large number of assets in this group have critical severity issues, which could mean that your organization may be exploited soon and have dire implications.
N/A	N/A	Asset is inactive and therefore has no effect on the security of your attack surface.

How CyCognito Enhanced Severity Scoring System is Calculated

A manual approach to issue prioritization is time-consuming and error-prone. Strapped for time, security teams often use the data at hand to make decisions (or none at all), creating unnecessary work and propagating a reactive workflow.

CyCognito scores and grades are dynamically created based on business context, test results and threat intelligence results. Assets start with a perfect score (100), which is then reduced based on calculated risk values. The logic is as follows, with example numbers.

INITIAL SECURITY SCORE		DISCOVERABILITY		ATTRACTIVENESS		ISSUE SEVERITY		FINAL SCORE / GRADE
100	-	5	-	7	-	13	=	75 B

CyCognito provides enhanced scoring and grading for more than just assets. Groups of assets also have scores, allowing an assessment of the collective risk of asset groups, such as organizations or subsidiaries.

The collective score is based on a weighted average of individual asset scores. Users can adjust group scores to be either strict (emphasis is on the worst-performing asset) or lenient (assets that are not the worst-performing). This allows organizations to tune scores based on their internal approach to risk measurement.

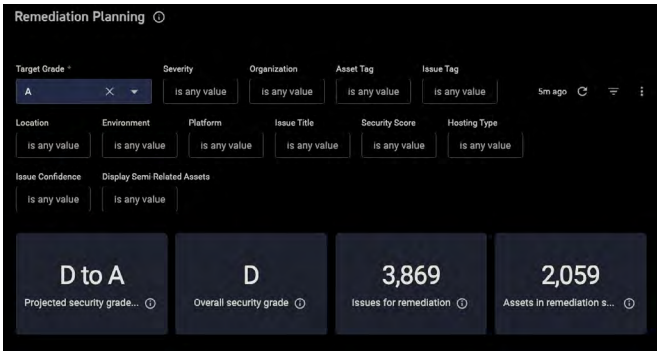
Remediation Planning and Exposure Scoping

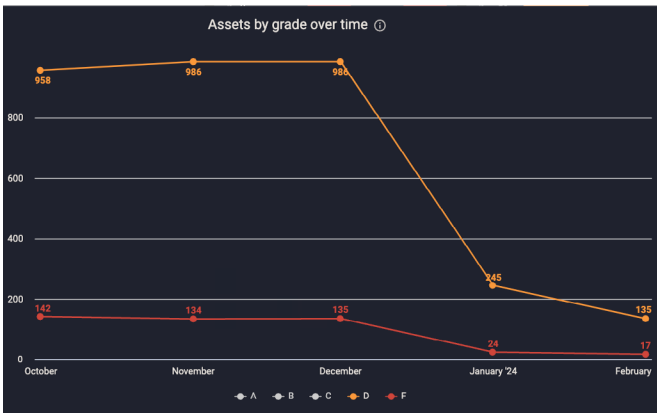
What is your desired risk exposure?

Consistently addressing your top issues will reduce your overall risk over time. However, planning is often required to understand the scope of work, setting expectations and making appropriate staffing decisions.

CyCognito's remediation planning dashboard allows you to build an action plan that targets specific exposure scopes based on inputs that include grade, organization, location, platform, and more. Output is a specific list of assets with issues to remediate, the organization that owns it and instructions on how to do it.

Graphical remediation progress tracking allows you to observe progress on the goals you set.





Comparing Issue Prioritization Approaches

Traditional prioritization requires heavy manual effort or an over-dependence on assumed data. CyCognito prioritization is fully automated and based on high-confidence security testing, business context and integrated threat intelligence to ensure the highest accuracy. Your SecOps team always works at its fullest potential on issues that matter.

Feature	Traditional Approaches	CyCognito
External asset inventory	Typically manually updated, often missing 30-50% of actual exposed assets due to a reliance on known IP ranges and domains.	Dynamically built list of globally externally exposed assets, across all IP ranges, subsidiaries, and domains, created without manual input or prior knowledge.
Business context	Typically not available other than for a short list of believed business-critical apps.	Broad range of risk-based context including asset attractiveness and discoverability, asset purpose for all assets in the external inventory.
Security testing	Typically not available; most security insight is provided by low-confidence vulnerability scanners. Pen testing provides higher accuracy but is infrequent, low coverage and difficult to operationalize.	Tens of thousands of high-confidence active security tests are run at the cadence of your choice across the entire asset inventory, including DAST for web applications.
Threat intelligence	Typically none, but if available, it is on an incomplete list of assets and based on low confidence port scan results.	Integrated threat intelligence offers a view into exploit weaponization and threat campaigns that are targeting assets like yours.
Scoring & grading	Typically based solely on CVSS scores, managed by spreadsheet.	Risk-based scoring based on a wide range of high confidence business, technical and security context, ranked and sorted automatically.
Remediation effort and validation	Not included.	Estimated effort to complete the included remediation steps are provided. Issues that are remediated are automatically retested to validate success.
Automation	Typically low, most context must be manually added or it's simply not used.	Fully automated prioritization workflow, reducing mean time to remediation.

FIND OUT MORE

Learn More about How CyCognito Helps Accelerate Prioritization Workflows

Build confident issue remediation workflows that include data you can count on. CyCognito's fully automated issue prioritization and remediation workflows reduce an operationally complex workflow to a simple service model.

If you are not a CyCognito customer and want to find out more about how we can help enable automated industry-leading prioritization across your full external attack surface, please contact us at info@cycognito.com.

Scalable, continuous, and comprehensive issue prioritization – only from CyCognito.