CYCOGNITO

EXECUTIVE BRIEF

ASSESS YOUR SECURITY EFFECTIVENESS

Best Practices in Five Key Steps

Conducting an organizational self-assessment of the strengths and weaknesses of your cybersecurity program is a critical process that should be an ongoing activity for every organization.

By establishing a baseline security evaluation of your cybersecurity effectiveness, you can measure your progress over time and implement plans to better align your program to your business priorities. This helps you improve your security program and ensure that investments in people and technology are aligned with your organizational priorities. There are five critical steps for an effective security self-assessment:

01

Start with an "outside in" view

Get an objective, informed view of your exposure to outside threats with an "outside in" view that looks at your organization from an attacker's point of view.

02

Assess your entire attack surface

Assess the attack surface for your entire IT ecosystem, which includes all attacker-exposed assets, known and unknown, wherever they are: on-premises, in the cloud, in third-party environments, or in your subsidiaries.

03

Measure status and identify critical risks

Establish the business context of your assets and their associated risks in order to evaluate the status of your current security program, identify the most critical risks to address first, and develop a remediation plan based on your organizational priorities.

04

Monitor continuously

Implement ongoing, continuous monitoring to maintain visibility to your changing attack surface and key risks.

05

Track KPIs

Track key performance indicators (KPIs) to measure your internal progress toward both long-term and short-term security goals.

Continuously looking from the outside in, and across your entire IT ecosystem, provides a full view of your attack surface that includes security blind spots, or *shadow risk*, which is where the greatest exposure often lies. A comprehensive view, when based on an assessment of each individual IT asset in your attack surface, allows grading of your organization's cybersecurity posture not only at the top level, but by its components.

Understand and Improve Your Cybersecurity Posture

The CyCognito platform helps you fully understand and measurably improve your cybersecurity effectiveness in alignment with industry best practices. It helps you determine if your cybersecurity exposure is aligned with your organization's risk appetite and quickly determine if you are investing too much time, money or resources protecting assets of little value or under-protecting priceless intellectual property or customer data.

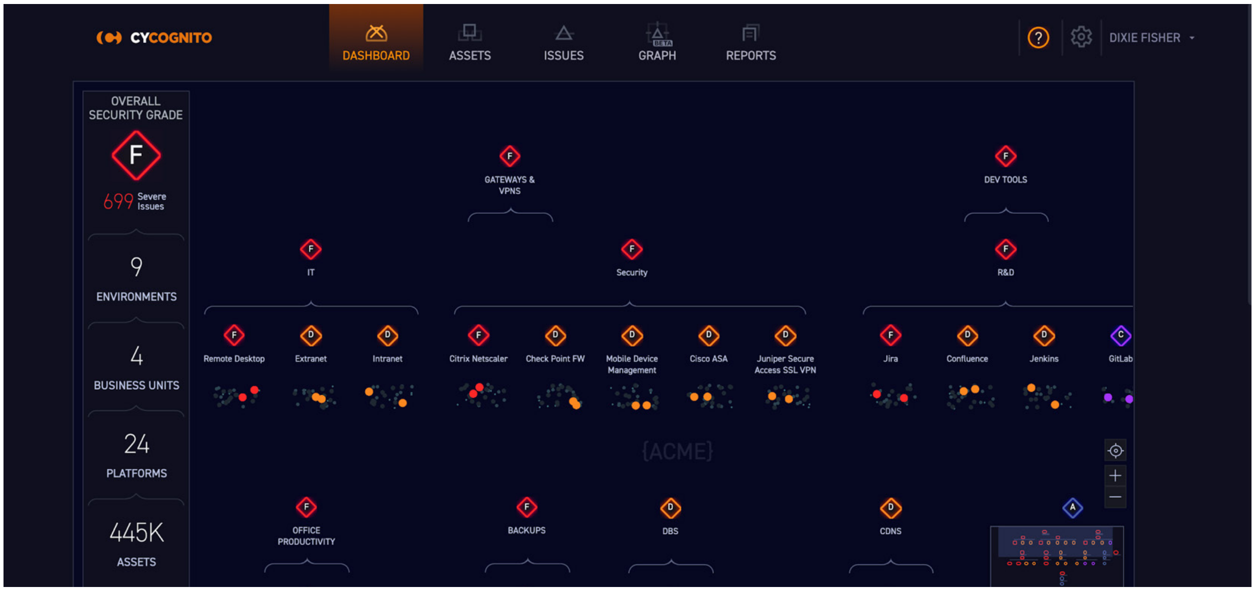

Figure 1. The CyCognito platform grades your security effectiveness, providing a summary score that is supported by detailed analysis and a score for each attack surface component.

Unlike legacy approaches and security ratings services that give you an incomplete view of your risk, the CyCognito platform helps you validate your security posture automatically and autonomously on a continuous basis. That helps you identify, prioritize and eliminate your most critical risks.

The CyCognito platform:

01 **Applies nation-state level cyber reconnaissance techniques to discover your attack surface:** Gives you an objective, “outside in” perspective of your organization from a sophisticated attacker’s point of view. This provides the full visibility and objectivity you need in order to set a baseline from which your program can evolve.

02 **Identifies risks across your entire IT ecosystem, including risks that legacy tools miss:** Assesses the attack surface for your entire IT ecosystem, including assets in on-premises, cloud, partner and subsidiary environments. This gives you confidence that you know where your most critical digital assets are and whether they are adequately protected.

03 **Measures your security status based on detailed analysis and offers actionable remediation:** Grades your overall security risk, built upon a detailed analysis of the business context and risk related to each individual IT asset in your attack surface. Supported by details for each of your attacker-exposed assets, it identifies the most critical risks that should be addressed first and offers specific remediation guidance.

04 **Monitors continuously:** Continuously monitors your attacker-exposed assets so that you have constant visibility to your changing attack surface and key risks.

05 **Creates reports to help you track KPIs:** Provides reports that you can use in conjunction with your KPIs to help you track your internal progress toward both long-term and short-term security goals.

To learn more about how the CyCognito platform can provide you with automated, cost-effective security self-assessment, contact us at *cycognito.com*.

CYCOGNITO
420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito is solving one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization, where they are most likely to break in, and how you can eliminate that risk.