NEDBANK

cymulate

Nedbank Increases the Breadth & Depth of its Cybersecurity Assessments with Cymulate

CASE STUDY

Challenge

Nedbank, one of the four biggest banks in South Africa, needs to protect itself and its subsidiaries from cyber threats and vulnerabilities that target the financial services industry. The Nedbank cybersecurity team wanted to replace its manual, resource-heavy cybersecurity processes to improve its protection from the latest active threats.

The team wanted a tool that could help them:

- **Automate security testing**
  The team was using up a lot of time and resources to develop assessments and manually run each one in its different environments and subsidiaries. Additionally, the team needed to ensure that the assessments were safe to run and would not harm the organization.
- **Track and detect drift**
  With different teams adjusting the security settings, the cybersecurity team did not have a centralized platform that could track those changes and ensure that none of them put the organization at risk.

The Cymulate Solution

Nedbank evaluated different security validation platforms based on technical, design, and user management requirements, and it also compared reporting, alerts, and vendor support. When the security team first witnessed Cymulate in action, Kevin Roberts, Information Security Analyst, recalled, **"From the moment we saw the Cymulate demo, we knew that if the product could do what the sales rep said it could, then it would be a perfect fit."**

During the onboarding process, Cymulate seamlessly converted Nedbank's evaluation instance into a production instance so the team could carry on from where they left off in the evaluation.

> Cymulate highlights your organization's security gaps so your team can work together to close them before an attack occurs.
> — Kevin Roberts, Information Security Analyst

Overview

Industry	Financial Services
HQ	Gauteng, South Africa
Company Size	30K+ employees

Solution

- Breach and attack simulation (BAS)
- BAS advanced scenarios

Results

- Ran over 130 assessments in less than 2 months
- Automate security validation on-prem and in the cloud
- Baseline and detect drift

Kevin explained that the security team uses Cymulate for:

Continuous control validation across the organization

"You can configure your security solutions to the best of your ability, but you can't just trust that they will protect you from all the threats out there. Cymulate allows us to validate that our solutions are tuned correctly and that we can do this continuously in different environments."

Production-safe assessments

"With Cymulate, all you need to do is configure an assessment and run it on the platform. You can trust the source of the tools used in the assessment and know that it's safe to run in your production environment."

Cloud security validation

"With our recent increased adoption of cloud environments, we use Cymulate BAS Advanced Scenarios to ensure all our cloud controls are working as expected."

Threat intelligence assessments

"Instead of chasing after the latest threat, the Cymulate research team keeps us up to date with emerging threat assessments so we can immediately evaluate our security and know if we are protected. We automatically run the immediate threats assessments daily."

Drift monitoring and detection

"Just last week, we discovered that a specific control in our subsidiaries' security stack was not aligned with our security control standards. Without Cymulate, we would have never been able to detect this kind of drift."

Vulnerability prioritization

"Cymulate helps us prioritize exploitable vulnerabilities in our environment. By integrating with our vulnerability management products and running Cymulate assessments, we can easily discover which vulnerabilities are an actual threat to our organization."

Benefits

- **Increased productivity** — The Nedbank team can run more assessments than ever before. In a two-month period, they were able to run 130 assessments.
- **Better allocation of resources** — With Cymulate, the Nedbank team knows which controls are working and which ones need to be improved so it can focus its time and resources on improving its security.
- **More comprehensive testing** — Cymulate provides the Nedbank security team with an extensive library of threat intelligence-led risk assessments that are simple to deploy and regularly updated, enabling the team to test its security more extensively than it was able to manually do before.
- **Automated IOC mitigation** — Cymulate seamlessly integrates with Nedbank's security controls to enhance the speed and accuracy of threat detection and response. The Cymulate IOC (indicators of compromise) mitigation capability automatically uploads critical IOC data directly to Nedbank's relevant security controls to ensure that potential threats are identified and addressed quickly.
- **Excellent customer service** — Since the start of its POC in 2022 until today, Nedbank appreciates the personalized support it receives from the Cymulate team to help optimize its use of the platform.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.