Cymulate

CASE STUDY

GUD Establishes Cyber Metrics Across 17 Subsidiaries with Cymulate

Challenge

GUD Holdings Limited owns a portfolio of 17 companies in the automotive aftermarket and water products sectors. The organization's small cybersecurity team is responsible for all the organization's subsidiaries, protecting office infrastructure, server infrastructure, information assets, and manufacturing equipment. The team outsources most of its security activities, including its security operations center (SOC), which monitors each business 24/7.

The security team faced the following challenges:

- Securing manufacturing equipment was especially difficult for the team because patching and maintenance often required scheduled downtime and business disruption.
- GUD would conduct sporadic third-party pen testing and basic vulnerability scanning to validate its security program, but these assessments only provided point-in-time snapshots that were quickly outdated.
- The security team had difficulty applying standard security metrics across all the business units and was unable to accurately report the efficacy of incumbent security controls across differing businesses within the portfolio.

GUD Head of Cybersecurity Shaun Curtis searched for a solution that could provide an ongoing and consistent assessment of the GUD cybersecurity posture across the entire organization, even with limited resources and expertise. It was important to Shaun to find one comprehensive tool that reduced cyber risk while increasing operational efficiency.

The Cymulate Solution

After considering numerous tools for security control validation, GUD selected Cymulate Breach and Attack Simulation (BAS) because of its simple implementation across the entire organization, ease of use, and ability to provide the same business metrics throughout all 17 subsidiaries. The smooth deployment enabled GUD to roll out the solution quickly across all its businesses.

Overview

Industry: Manufacturing
HQ: Melbourne, Australia
Company Size: 501-1k employees

"With Cymulate, we can measure our infrastructure and our security controls automatically against the latest and most pervasive threats from one platform and get a metric which is consumable by leadership."

- Shaun Curtis, Head of Cybersecurity

Solution

Breach and Attack Simulation (BAS)

Results

Establish metrics across 17 subsidiaries

Validate security against emergent threats

Detect drift and optimize defenses

Shaun elaborated that the security team uses Cymulate to:

Test against emergent threats
"As a manufacturing organization, we need to be on top of ransomware attacks. With Cymulate Immediate Threats Intelligence, we're ahead of the curve and don't need to wait for authorities to provide us with intel about emerging threats."

Gain insights into exposure risk
"Cymulate BAS provides insights into exposure risk that vulnerability scanners cannot deliver. Basic vulnerability scans tell you where you're vulnerable, but Cymulate tells you if you will be compromised. Vulnerability scanning just gives a report. Cymulate gives us intelligence."

Measure the security efficacy of each business in a consistent manner
"My team can compare the performance of different businesses using the same security controls, identify discrepancies, and address security issues more effectively. With Cymulate, we can run security assessments and quickly develop a metric across our entire business—something that would take me hours to do manually."

Evaluate new tools
"We use Cymulate BAS to assess new technologies during the proof-of-concept stage. My team runs Cymulate attack simulations against the new product to see if the vendor can protect GUD as well as it guarantees it can."

Benefits

- **Benchmark and improve cyber performance** – The Cymulate dashboard shows individual risk scores per security control based on the most recent assessments. Using the Cymulate risk scores, GUD established a benchmark for each control so that if one of the subsidiaries drops below this score, the security team focuses its resources on bringing that score back up.
- **Identify areas of improvement** – Cymulate BAS helps the team identify configuration issues and security gaps that would have gone unnoticed. Early in the platform's deployment, Cymulate highlighted the ineffectiveness of one security control that was used across all the GUD business units. With this intelligence, GUD evaluated the control's configuration and prioritized changing the technology to enhance security.
- **Enhance communication and reporting** – The security team includes Cymulate BAS metrics and analytics in its monthly report to communicate to leadership each business's cyber performance. These analytics help the board understand the importance of cybersecurity and facilitate discussions around budget allocation and return on investment (ROI) for security initiatives.

Plans for the Future

After seeing the benefits of Cymulate BAS, the GUD team has plans to expand its security validation and exposure management program with Cymulate Attack Surface Management (ASM) and Continuous Automated Red Teaming (CART). One of the main reasons GUD chose Cymulate was that it could grow along with the platform and utilize its more advanced solutions as it sees a need for them. Shaun also appreciates that Cymulate invests a lot in the research and development of the platform, and he has faith that its capabilities will only continue to expand and improve in the future.