Cymulate

GUD Establishes Cyber Metrics Across 17 Subsidiaries with Cymulate

Overview

About GUD Holdings Limited

GUD Holdings Limited operates a portfolio of seventeen companies in the automotive aftermarket and water products sectors. Its principal markets are Australia and New Zealand.

Challenge

The GUD security team was unable to apply standard security metrics and measure the efficacy of its security controls across its 17 subsidiaries.

Solution

GUD utilizes Cymulate BAS to streamline and automate its security testing and measure the security efficacy of each business in a consistent manner across all its business units.

Benefits

GUD benchmarks cyber performance for each subsidiary, identifies areas of security that need improvement, and benchmarks results for communication with leadership

> *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

Challenge

The small GUD cybersecurity team is responsible for all 17 of the organization's subsidiaries, protecting office infrastructure, server infrastructure, information assets, and manufacturing equipment. Securing manufacturing equipment is especially difficult because patching and maintenance often require scheduled down time and business disruption.

The team outsources most of its security activities, including its security operations center (SOC), which monitors each business 24/7. 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to validate its security program, but these assessments only provided point-in-time snapshots that were quickly outdated.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 team needed a way to validate its security controls in a continuous and automated fashion.

Although each business unit has more or less the same security stack, the security team had difficulty applying standard security metrics across all the business units. Additionally, without tangible metrics, the team 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. Curtis said, **"I could buy a whole bunch of tools to validate my controls across the organization, but I don't have the time, bandwidth, or expertise to do it continuously with numerous tools."** It was important to Curtis 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 seventeen subsidiaries. Curtis remembered using the platform for the first time:

> *The Cymulate proof of concept was great. It opened our eyes to what we could achieve, and I liked the simplicity of the metrics.*

The smooth deployment enabled GUD to roll out the solution quickly across all its businesses.

GUD utilizes Cymulate BAS to streamline and automate its security testing processes, saving significant time and resources for the security team. As manufacturing organizations are known targets for ransomware attacks, GUD is kept up to date on the latest threats with the Cymulate BAS immediate threats intelligence capability. GUD receives out-of-the-box assessments against new threats as they emerge, effortlessly testing its defenses against them. Curtis added, **“With Cymulate Immediate Threats Intelligence, we're actually ahead of the curve and don’t need to wait for authorities to provide us with intel about emerging threats.”** The technical team uses the Cymulate CSV reports and remediation guidance to analyze and fine-tune its security measures.

Since implementing Cymulate, GUD reserves manual pen testing for specific, targeted testing because the team can run its own automated assessments whenever it needs. Additionally, Cymulate BAS provides GUD with insights into exposure risk that vulnerability scanners cannot deliver. Curtis said, **“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.”**

With Cymulate BAS, GUD measures the security efficacy of each business in a consistent manner. The security team can compare the performance of different businesses using the same security controls, identify discrepancies, and address security issues more effectively. Curtis explained, **“Our vision is that every business has the same set of security controls with the same metrics, and Cymulate is helping us accomplish this. 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.”**

Curtis has also seen an improvement in how GUD engineers approach cybersecurity. He said,

> *Now that we can inspect and measure security efficacy across the businesses, the engineers actually want to know how effective their environment is.*

GUD also uses Cymulate BAS to assess new technologies during the proof-of-concept stage. The team runs Cymulate attack simulations against the new product to see if the vendor can protect GUD as well as it guarantees it can.

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. Curtis 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.

Benefits

Cymulate BAS provides the following additional benefits for the GUD security team:

Benchmark 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. The team also used Cymulate when evaluating which tool was the best replacement for the underperforming security control.

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. Curtis said, **"With Cymulate, we can present tangible metrics to the board about the efficacy of our security program."** These analytics help the board understand the importance of cybersecurity and facilitate discussions around budget allocation and return on investment (ROI) for security initiatives.

About Cymulate

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and to gain evidence for compliance and regulatory purposes.