cymulate

CASE STUDY

GUD Gains Control of its Attack Surface Across 17 Subsidiaries with Cymulate ASM

Challenge

After hardening its security posture with automated security validation, GUD Holdings Limited tackled the next challenge of taking control of its attack surface.

Operating 17 portfolio companies in the automotive aftermarket and water products sectors, GUD relies on a small security team and automated offensive security testing from Cymulate. GUD measures the security efficacy of each business consistently across all its business units with Cymulate Breach and Attack Simulation (BAS) and Cymulate Continuous Automated Red Teaming (CART) (read more).

When Shaun Curtis, Head of Cybersecurity, wanted to take control of the organization's attack surface, he again looked to Cymulate. With responsibility across the 17 subsidiaries, Shaun and his small team recognized the need to keep track of each business unit's external assets. This unmonitored external attack surface could expose the organization to social engineering attacks or unauthorized network access, establishing a foothold within the organization.

The security team used open-source tools to scan for and manage its assets, but it was very labor-intensive and time-consuming. Shaun wanted an exposure assessment solution that could:

- Discover all assets associated with GUD's infrastructure
- Provide additional information about vulnerabilities and misconfigurations related to the found assets
- Show the relationship between GUD's internal infrastructure and its external assets.

The Cymulate Solution

After successful deployments of Cymulate BAS and Cymulate CART, Shaun saw the value in a consolidated exposure validation platform, but he was unwilling to sacrifice function for attack surface visibility. Cymulate Attack Surface Management (ASM) delivered both.

Shaun elaborated, **"I chose to implement Cymulate ASM because I wanted intelligence on my assets, not just a long list of vulnerabilities that a vulnerability management tool would give me."**

Overview

Industry	Manufacturing
HQ	Australia
Company Size	501-1k employees

> Cymulate ASM was simple to implement, but it added so much value to our cybersecurity.
>
> — Shaun Curtis
> Head of Cybersecurity

Solution

- Attack surface management

Results

- Risk prioritization
- Continuous monitoring of the attack surface
- Discovery of unknown external assets

Implementation was simple. The security team provided one domain, and Cymulate ASM automatically found all its additional related domains. Each GUD business unit uses Cymulate ASM to automate two types of scans: One to discover assets (weekly) and one to detect vulnerabilities and misconfigurations against those found assets (monthly).

Shaun explained that the GUD team uses Cymulate ASM for:

A centralized view of all its external assets

"Cymulate ASM gives us a consolidated view of all our external assets, per business, in one place."

Actionable guidance

"The Cymulate ASM list of external assets includes information on which assets are exposed, their severity, when they were first seen, mitigation recommendations, and more. We can take these insights to the business units and plan a strategy around how to execute against those findings."

Benefits

- **Awareness** — The business units now understand the risks of exposed external assets and consider this when deciding to onboard new vendors.
- **Automation** — The small security team maintains control and visibility over its attack surface with automated scans.
- **Prioritization** — With valuable insights into GUD's IT infrastructure, the team prioritizes and addresses potential risks to strengthen its security posture.
- **Consolidation** — Because Cymulate provides a consolidated platform with many capabilities, GUD was able to add Cymulate ASM without adding an entirely separate vendor to its security stack. One of the main reasons GUD chose the Cymulate platform was that GUD could grow along with the platform and utilize its more advanced solutions as it saw a need for them.

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.