LV= Takes a Data-Driven Approach to Cybersecurity with Cymulate

CASE STUDY

Challenge

Dan Baylis joined LV= in 2022 as Chief Information Security and Data Officer and quickly identified that the cybersecurity team lacked the required analysis of its security posture to drive data-driven conversations around its security. With an in-house staff of 10, an outsourced 24×7 SOC provider and third-party specialists for pen tests and red team exercises, the LV= cyber program was missing the data and insights that Dan needed to measure how defenses and processes minimize exposure.

Dan and LV= faced challenges common to many cyber programs:

- **Lacked continuous security validation**
  LV= conducted annual penetration tests like most other organizations, but the results provided point-in-time snapshots of the organization's security posture.
- **Labor-intensive and time-consuming testing of emergent threats**
  The process to validate against emerging threats was extremely inefficient. It included manually researching the threat's IOCs, testing controls against the IoCs, implementing any control changes if the threat did get through, and repeatably retesting to validate the mitigation.
- **No consolidated view of security posture**
  LV= was using security tools that were not integrated with one another. Additionally, the security team had difficulty aggregating all the information it received from its third-party SOC and red team vendors, causing everyone to work in silos.

The Cymulate Solution

LV= needed a solution that could be easily implemented and provide the organization with continuous security control validation, metrics, and reporting. Dan recalled, **"When I joined LV=, Cymulate was the first vendor I added to our security stack. We required a solution that works. As a previous user, the product speaks for itself."** The Cymulate products were easy to configure and integrated with the team's existing security stack to provide a consolidated view of all its security activities.

> Cymulate enables us to have data-driven conversations about cybersecurity. No more opinions. It's just the facts.
>
> Dan Baylis, Chief Information Security and Data Officer

Overview

Industry	Financial Services
HQ	UK
Company Size	1k-5k employees

Results

- Continuously validate security controls
- Reduce time and effort to evaluate emergent threats
- Baseline and improve security

Benefits

- Increased data-driven conversations about security controls
- Empowered SecOps that drive real improvement
- Increased efficiency
- Validated investments

The LV= team continues to appreciate the support they receive from the Cymulate customer success team. Karl Ward, Head of Cybersecurity, elaborates, "The fast turnaround from the Cymulate support team is key. It is key to have a technical account manager who understands the tool and helps us maximize its capabilities."

The LV= team uses Cymulate to:

Continuously validate security controls

"Cymulate allows us to continuously confirm if our security controls are resilient, and it gives us data-driven answers."
— Dan Baylis, Chief Information Security and Data Officer

Immediately assess against emergent threats

"The Cymulate Threat Research Group is always quick to create new emerging threat assessments. With minimal effort, we understand our exposure and how to mitigate it."
— Adam Boden, Lead Cybersecurity Operations Specialist

Quantify risk exposure to baseline and improve security

"We use the Cymulate reporting to track our improvement over time. We present this data visually to stakeholders who are not security experts in a way they can understand."
— Dan Baylis,. Chief Information Security and Data Officer

Finetune tools with remediation guidance

"Using the Cymulate integrations, we launch assessments to see if our tools detect them. If they don't, Cymulate provides mitigation guidance and Sigma rules, and we easily rerun the assessments to validate remediation."
— Karl Ward, Head of Cybersecurity

Benefits

Since implementing Cymulate, the LV= security team has noted significant improvements to its security organization.

- **Increased data-driven conversations about security controls** — Cymulate provides facts and data regarding how safe LV= is against threats, and this information leads all its security conversations.
- **Empowered SecOps that drive real improvement** — The platform's automation and real-world attack assessments create engaging projects that expand skills and keep SecOps employees motivated.
- **Increased efficiency** — The support of the Cymulate Threat Research Group and the automation for repeatable and accurate testing eliminates the need for more security professionals to scale activities.
- **Validated investments** — The security team uses Cymulate's reporting to show stakeholders risk reduction after implementing new tools.