cymulate

Law Enforcement Agency Restores Confidence in Cyber Defenses with Cymulate

CASE STUDY

Strong Cyber Defenses Required to Bring Criminals to Justice

As one of the UK's leading law enforcement organizations, this agency plays a critical role in both local policing and nationwide crime prevention initiatives. With responsibility for safeguarding fraud services and protecting sensitive digital evidence tied to criminal investigations, its lean cybersecurity team faces a demanding mission: securing critical systems and data that enable officers to operate effectively, investigate crimes and bring offenders to justice.

However, the security team wasn't confident that its security controls would protect the organization in case of cyberattack because:

- **The team could not continuously validate its controls.**
  While the team conducted its required annual penetration tests, they were manual, limited in scope and provided only a point-in-time assessment.
- **It was challenging to ensure protection against emergent threats.**
  The security team could not independently test its security against new threats in the wild. Instead, it had to ask its IT team to test the controls, taking anywhere from two days to a week before it could determine whether the controls needed remediation.
- **The team could not keep up with patching its vulnerabilities.**
  The team would run vulnerability scans but did not know how to prioritize the long list of critical vulnerabilities that were consistently found.

Like many small security teams, this team first considered outsourcing its security validation and regular testing, but it quickly recognized that this would be costly and wouldn't give the team the visibility and independence it required. The organization's CISO began investigating automated security validation tools such as breach and attack simulation (BAS).

The Cymulate Solution

The CISO determined that Cymulate was the ideal solution to empower his team. He reflected, **"Back in 2019, we were one of the first organizations in the UK to use Cymulate. I thought the product was very innovative and has continued to meet my expectations. Looking back, I truly appreciate how our security organization has matured alongside the product."**

> "Cymulate gives me the confidence that I know what's going on in my security stack. It doesn't just provide me with security validation, it allows me to look over the horizon at the next biggest potential threat."
> – CISO

Overview

Industry	Law Enforcement
HQ	EMEA
Company Size	1K-2K employees

Use Case

- Threat Validation
- Control Optimization
- Exposure Prioritization & Mitigation

Results

- Continuously validate security
- Ensure protection against new threats
- Prioritize based on validated risk
- Increase efficiency

Today, the security team uses Cymulate to continuously validate and improve its security posture by managing control drift, staying ahead of emerging threats, automating IoC mitigation, prioritizing exploitable vulnerabilities and proving the impact of security investments.

Detect and manage drift

"We initially used Cymulate to fine-tune and optimize our security controls. Today, our risk score is very low for each control, so we can focus on managing our drift. Now, we run assessments automatically every week, review the output in the Mitigation Hub, prioritize the required mitigation actions, remediate when necessary and then retest. If Cymulate flags something, we know to address it quickly."
- Information security manager

Validate against emerging threats

"As soon as I hear of a new threat, I send that information to my team to understand if the organization is exposed. The team often responds that it automatically tested for the threat last week with Cymulate and reports on the steps it took if remediation was necessary. We're always ahead of the game with Cymulate."
– CISO

Automate IoC mitigation

"Cymulate Auto Mitigation automatically pulls IoCs from validated attack simulations and pushes them straight into our security controls. It then re-runs the assessment to prove the threat is actually blocked. We also use the platform's IoC data to strengthen other security products that may not yet have identified those IoCs or hashes."
– Information security manager

Prioritize vulnerabilities

"Through validation, Cymulate helps us understand which vulnerabilities can be exploited in our organization. This helps us focus our limited resources so we can be proactive and remediate before a threat becomes an actual problem."
– CISO

Manage and prove investments

"With Cymulate, I have the evidence to direct and manage my resources. For example, if I see a gap, I know where I need to invest more resources to keep our organization safe, and I can show the results of that investment."
– CISO

Benefits

- **Independence.** With Cymulate, the team can independently test its security and run assessments whenever needed without waiting for an annual penetration test.
- **Increased efficiency.** The platform's automation, along with Cymulate Vero AI, enables the small team to increase its validation activities and strengthen its security posture.
- **Threat intelligence.** With continuous updates from the Cymulate Threat Labs, the security team leverages this threat intelligence within and beyond the platform to bolster their defenses.