Raiffeisen Bank International

Cymulate

CASE STUDY

RBI Validates and Optimizes SIEM Detection with Cymulate

Challenge

Over the past five years, Raiffeisen Bank International (RBI) has invested heavily in cybersecurity, increasing security staff, tooling, and infrastructure at its head office in Vienna, including the creation of its own Raiffeisen Cyber Defense Center (RCDC). With the cybersecurity department growing in size and maturity, the RCDC team understood that manual testing and internal response exercises alone were not enough to validate the organization's detection and response capabilities continuously. The team began to experience the following challenges:

- **High effort to continually test and validate its SIEM**
  The RCDC team relied heavily on industry standards and best practices to write detection rules but could only validate their efficacy based on historical logs or manual testing. However, when writing new detection rules to target highly specific malicious behavior, the team could not validate whether the detection rules would detect what the team intended.

- **Complexity of keeping up with emerging threats**
  With new daily threats, the team could not keep up with manually testing its defenses and ensuring its controls were protecting the organization.

- **Difficult to conduct internal incident response exercises**
  Besides regular penetration tests and red teaming activities, the RCDC team was looking for a more streamlined way to challenge its internal response mechanisms, especially on an ad-hoc basis, to evaluate if everyone would follow the appropriate procedures and protocols in the face of an attack.

The Cymulate Solution

RBI searched for a security detection validation tool, and after evaluating the different vendors in the market, RBI decided to implement Cymulate. The team appreciated that Cymulate provided integrations with tools already in its security stack, and the simple agent deployment. Additionally, Cymulate offers many capabilities to support SIEM validation and detection engineering.

Markus Flatscher, Senior Security Manager, elaborated on the different ways his team utilizes the Cymulate platform:

> **Validate SIEM detection**
> "When we create a new detection rule in our SIEM that we can't validate with historical logs, we use Cymulate assessments to generate the appropriate events and see if the rule was successful in its detection. The immediate feedback is useful when fine-tuning our SIEM and practicing detection engineering."

Overview
Industry: Banking
HQ: Vienna
Company Size: 10K+

> "Cymulate is one of the only tools I know that can show internal stakeholders who have no knowledge of cybersecurity why cybersecurity is important and something worth investing in."

Markus Flatscher, Senior Security Manager

Solution

- Breach and attack simulation
- BAS Advanced Scenarios
- Automated Network Pen Testing (Hopper)

Results

- SIEM validation
- Operationalize the MITRE ATT&CK framework
- Improved communication with stakeholders

Ensure protection against emergent threats
"If we wanted to test against emergent threats before, it was all manual. Cymulate provides us with one curated list of IoCs, which we distribute to our EDR and web gateway to ensure we are protected against these new threats in the wild."

Execute incident response exercises
"We are starting to use Cymulate for our incident response exercises, and we appreciate that we can customize the assessments directly to our needs. For example, we are creating attacks with chained activities that are suspicious enough that they will require investigation and validate that the team knows how to act and follow internal processes."

Run both out-of-the-box and customizable assessments
"With Cymulate, we have many tests that we can run out of the box, like immediate threats assessments, endpoint security assessments, and APT-focused advanced scenarios. But we also can highly customize chained assessments—we decide what we want to run, how we want to run it, and where we want to run it."

Operationalize the MITRE ATT&CK framework
"The Cymulate MITRE ATT&CK Heatmap helps us easily visualize our gaps and coverage of the MITRE framework. We quickly understand if there are specific MITRE techniques or sub-techniques that we haven't been able to detect, so we know exactly where we need to allocate our resources for better protection."

Improve communication with stakeholders
"On the one hand, Cymulate enables you to validate your security controls easily, but it also provides you the results in a digestible manner to use when communicating with internal stakeholders."

Benefits

- **Increased efficiency** – RBI quickly validates new detection rules with a few clicks.
- **Improved security** – The security team can create a benchmark of its cyber security performance and understand what needs to be done to reduce risk continuously.
- **Ongoing customer support** – The onboarding process was quick and easy, and the RBI team appreciates the continued support from the Cymulate customer success team.

Plans for the Future

The RCDC team has plans to expand its use of the Cymulate platform for security validation of cloud-based workloads and continuous detection engineering and refinement, network segmentation validation both on-prem and in the cloud, and purple team automation.

Additionally, the RCDC team will roll out Cymulate to all of its internal customers, which are various legal entities spread across central and eastern Europe to replicate the success of its implementation at the bank's headquarters.