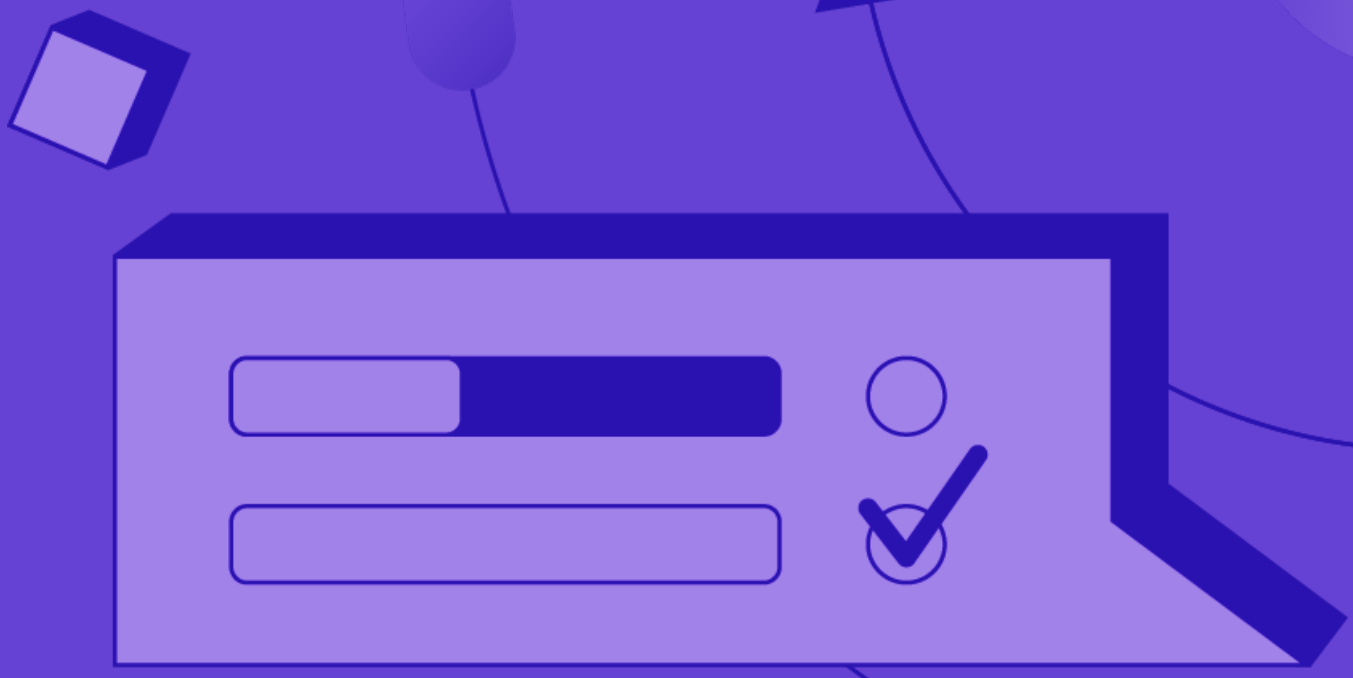
ATTACKIQ® + esed
CYBER SECURITY & IT SOLUTIONS

Case Study

ESED, a Spanish MSSP, Leverages AttackIQ to Provide Customers with Better Insights and Validate Security Control Effectiveness



Spanish managed security service provider (MSSP) ESED specializes in identifying gaps in customer companies' security controls. It attacks the controls that organizations have in place, then helps those businesses mitigate any problems that the attacks bring to light. This specialization reflects the mission the company has had since it was launched in 2010, when its founders saw a looming gap in the security capabilities between large and small businesses.

"The main idea behind the formation of ESED was that we saw big companies usually have a sufficient budget to invest in cybersecurity, but we often did not see the same investments in small businesses," explains Eduard Bardají Cros, Co-founder and CEO of ESED. *"Cyberattacks are as much of a threat to smaller companies as to large companies. ESED formed to solve the cybersecurity challenges, and protect business data, for small to midsize businesses."*

The Barcelona-based firm provides advisory services on everything from cybersecurity strategy to implementation of firewalls and endpoint protection to building a backup and data-recovery infrastructure. *"We have developed security expertise through our backgrounds working in major multinational companies,"* Bardají says. *"Now we channel this knowledge to introduce cybersecurity best practices into smaller businesses."*

Red teaming capabilities lie at the heart of ESED's service offerings. *"We call our penetration testing service ESED Attack,"* Bardají explains. *"We attack our customers' systems in order to find security vulnerabilities before the bad guys do."* ESED uses the cloud-based AttackIQ Security Optimization Platform to test and validate their clients' security program effectiveness with greater ease, scale, and effectiveness.

> ***"When we met AttackIQ, the game changed. We liked the flow of the AttackIQ platform, we liked the idea and the framework, and as soon as they showed us the platform, we were comfortable with it."***
>
> – Eduard Bardají Cros,
> Co-founder and CEO,
> ESED

Manual Pen Testing Is Tough to Scale

When first developed, ESED Attack presented significant operational challenges. The service consisted of penetration (pen) tests that were highly manual and time-consuming. *"The success of a pen test is related to several factors, including how many people it requires to run and how much time they have for performing the attacks,"* Bardají says. *"This meant our manual testing process was not really scalable. The more customers we had, the more people and time we needed to complete pen testing."*

CUSTOMER

ESED

LOCATION

Spain

INDUSTRY

Cybersecurity & IT Solutions

HIGHLIGHTED SOLUTION AREAS

- Security Control Validation
- Investment Decision Support

BUSINESS IMPACT

- Supports business growth by enabling the team to provide more control assessments in a shorter time frame
- Assessments require 50%–90% less staff time than manual penetration tests
- Enables ESED to respond in less than a week to customers' requests for urgent assessments, based on geopolitical developments or other timely events
- Underpins the new ESED Attack service offering, which provides five times more revenue vs. manual penetration testing
- Frees up more time for staff to design sophisticated attacks, as well as advise customers on best practices and remedies for discovered controls gaps
- Helps the small to mid-size businesses that are ESED customers strengthen their cybersecurity infrastructure

Manual Pen Testing Is Tough to Scale (cont.)

Qualified security professionals are in short supply in Europe, as elsewhere around the world. It was not feasible to add to the company's staff anytime demand temporarily surged. Thus, the limited number of people available to run cybersecurity assessments was limiting ESED's pen testing capacity. The ESED team's first solution to this challenge was to automate as many pen testing tasks as possible. They wrote scripts and built some in-house tools, but those did not completely solve the challenge.

"When we met AttackIQ, the game changed," Bardají says. In 2016, ESED leadership was introduced to members of the nascent AttackIQ team. They immediately bought into the concept of breach and attack simulation (BAS) software. *"This was a very early stage of the AttackIQ Security Optimization Platform, but we liked the flow of the AttackIQ platform, we liked the idea and the framework, and as soon as they showed us the platform, we were comfortable with it."*

Adds Guillem Raja, a junior cybersecurity technician with ESED, *"AttackIQ also stands out because even as it emulates the adversary in its testing process, we can be confident that if we attack a client's production systems, we will not break their workflows. That is a problem for some pen testing tools."*

AttackIQ in Action

Customers ask ESED to attack their cybersecurity infrastructure for a number of reasons: they want to find security gaps that they can patch with new tools or processes. They want to confirm that security fixes they have made are effective. They want to build the confidence of senior management that the controls they have in place can thwart specific threats their executives are concerned about. Or they want to justify their existing or projected future investments in security solutions. Across all these use cases, the AttackIQ Security Optimization Platform streamlines assessment processes.

When a customer approaches ESED with a specific testing need, the firm uses the MITRE ATT&CK framework to guide development of attack simulations. ATT&CK is a globally accessible knowledge base of adversary tactics and techniques that was built by the nonprofit MITRE Corporation based on security professionals' analyses of real-world cybersecurity incidents. ESED staff use the framework to determine which attacks, tactics, and techniques would best emulate the types of threats the customer is most concerned about.

> ***"It does not matter how many machines the customer wants to test. A large-scale simulation takes one-fourth or one-fifth as much time as it would take if we were performing the assessments manually."***
>
> – Alex Paredes Martinez,
> Senior Full-Stack Software Developer,
> ESED

"Even before working with AttackIQ, we were basing our pen testing decisions and our metrics on the MITRE ATT&CK framework," says Alex Paredes Martinez, ESED's senior full-stack software developer who focuses on cybersecurity. *"The tight integration of MITRE ATT&CK principles into the Security Optimization Platform is one of the things we liked about AttackIQ from the beginning."*

AttackIQ in Action (cont.)

Once the ESED team decides on an appropriate line of attack, they can either leverage attack scenario templates that come with the platform, or they can upload their own attacks. *"The ability to utilize our custom-built attacks was another thing we liked about the AttackIQ Security Optimization Platform,"* Paredes adds.

Bardají provides an example: *"One of the attack flows that we are frequently asked to simulate is the full ransomware attack vector. We need to see whether ransomware is likely to get into the network via an email or web download. But we also need to see, if ransomware does get in, whether it can move laterally within the network. We run a series of simulations in AttackIQ, and when we sum the results of these separate assessments, we have the full attack vector."*

The AttackIQ Security Optimization Platform streamlines this entire process compared with manual pen testing. *"Because it is so easy to launch an attack within the Security Optimization Platform, we can very quickly run these batches of attacks to understand whether there are any control gaps in the infrastructure,"* Bardají says. *"In one case, we developed an attack to test an aspect of the data loss prevention [DLP] system that one of our customers was running. Initial development of that assessment took a month. But now, we can replicate this same assessment in a couple of minutes."*

> ***"AttackIQ also stands out because even as it emulates the adversary in its testing process, we can be confident that if we attack a client's production systems, we will not break their workflows. That is a problem for some pen testing tools."***
>
> – Guillem Raja,
> Junior Cybersecurity Technician,
> ESED

In addition, using an automated attack simulation tool ensures consistency across assessments, which helps ensure that test results are targeting the right issues. *"We know that human error or human judgment did not lead to a change in any aspect of the attack from one simulation to another,"* Raja says. *"The only things that could have changed are the customer's production systems which we are assessing."*

After completing an attack simulation, ESED provides the customer with a report showing the results. The reports incorporate a dashboard that ESED created. The dashboard automatically pulls in test results using AttackIQ's reporting API. Bardají says the reports tend to be well-received by customers: *"The dashboard makes it easy to understand exactly where we found vulnerabilities, and customers generally tell us that the reports add a lot of value to our engagement."* Then, when they have provided the results via dashboard, the ESED team meets with the customer to help them understand the opportunities for improvement.

Automated Testing Saves Time Over Pen Testing

Working with AttackIQ gives ESED the ability to scale the business for faster growth. The lean team can respond more quickly to more customers' requests for security validations. *"If customers want to simulate an attack on hundreds of endpoints, AttackIQ enables us to complete those simulations in about the same length of time testing a single endpoint would take,"* Paredes says. *"It does not matter how many machines the customer wants to test. A large-scale simulation takes one-fourth or one-fifth as much time as it would take if we were performing the assessments manually."*

"As an example," Bardají adds, *"a couple of weeks ago, the Spanish division of a global company asked us to do a cybersecurity assessment across their 500 employees' endpoints. Because of the Russian war and other current events, they wanted to make sure they had the right security infrastructure in place. We ran 74 specifically chosen scenarios (attacks) across five critical targets in under a week. With a manual pen test, in the best-case scenario, the tests would have taken us at least three weeks, plus another week to generate a report on the results."* AttackIQ's Russian government-focused attack graphs allow security teams to test and validate their defense effectiveness against real-world adversary capabilities.

By automating attack graph tests and other assessments, the AttackIQ Security Optimization Platform enables ESED to provide ongoing assessments. *"One service option we offer is annual, quarterly, or monthly testing of the attack vectors that a customer is most concerned about,"* says Bardají. *"Such routine assessments would have been very difficult to offer in a manual pen testing environment."*

Perhaps most important to the success of ESED, the AttackIQ Security Optimization Platform frees up staff members for strategic activities. *"When we are not running the attacks manually, it is nice to spend that extra time thinking about what advice we should give to the customer, what the best strategy would be for them to deal with any control gaps we discovered,"* says Raja. ESED has improved its reporting system to make assessment results easier for customers to understand. The additional time freed up by automating attacks also enables ESED to develop new and more powerful attack scenarios.

Ultimately, Bardají concludes, *"the AttackIQ Security Optimization Platform enables us to do more testing in less time and with fewer people. It is a win-win situation."*

ATTACKIQ

U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Engenuity's Center for Threat Informed Defense

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.