Advantage | Mitre 10 | AttackIQ - Case Study

Protecting Mitre 10: Advantage delivers automated penetration testing with AttackIQ

Advantage®

About Advantage

As one of New Zealand's longest standing ICT and security providers, Advantage brings leading threat intelligence and frontline expertise to organisations.

ISO27001 and Incident Response SIREN certified, we are armed with the tools and skills to increase security effectiveness and reduce business risk.

To learn more about Advantage, visit:

advantage.nz

MITRE 10

About Mitre 10

Mitre 10 has been a part of New Zealand's home improvement culture since 1974. New Zealand owned and operated with stores across the country, Mitre 10 is a Kiwi success story and is New Zealand's most trusted home improvement and garden retailer.

To learn more about Mitre 10, visit:

mitre10.co.nz

Mitre 10 operations with Advantage

While essential in assuring the reliability and safety of the information technology systems powering trading, Mitre 10's penetration testing regime was manual, cumbersome, and therefore costly. When managed security services provider Advantage recommended an automated option powered by AttackIQ, the New Zealand-wide building supplies and home improvement retailer was quick to recognise the benefit. As a result, today Mitre 10 enjoys scheduled penetration testing on a continuous basis, rather than the previous 'point in time' approach, contributing to improved security, while those charged with risk management can focus their attention elsewhere.

Mitre 10 has been a part of New Zealand's home improvement culture since 1974. New Zealand owned and operated with stores across the country, Mitre 10 is a Kiwi success story and is New Zealand's most trusted home improvement and garden retailer. With a steadily growing trade business, Mitre 10 has expanded its supplier network in New Zealand and overseas, steadily building upon a competitive advantage, great pricing and increased range for customers.

Situation

As a co-operative with 84 independently owned stores around New Zealand, Mitre 10 and associated co-operative Hammer Hardware which comprises a further 60 stores, runs a federated model with shared services provided out of national support centre in Auckland. "From a security perspective this is a challenging environment as we don't mandate things but provide a series of menus from which our store owners can choose," notes Brad Ward Able, Mitre 10's Head of Security and Risk. "What works for one store might not work for another, so we always work to structure the services available to have broad appeal."

While in the process of a multi-year change programme introducing a new Enterprise Resource Planning solution for the back end and updating its Point-of-Sale infrastructure, Ward Able says an opportunity presented itself for the establishment of standardised security processes, fitting into the services menu. "Standardisation works because it offers benefits with scale, it's easier to roll out, and it is easier to support," he explains. "With every system that goes out, our process included penetration testing to be sure of the basics and that everything in the security stack is looked after, not leaving anything open. But this is expensive, manual, and slow. It's also only a 'point in time' test."

Advantage | Mitre 10 | AttackIQ - Case Study

This would take a tester a week, with a report coming a further two weeks later. Ward Able says Mitre 10 recognised these shortcomings and sought a better approach. "For me, that didn't really work. I needed automation specifically because we continuously have new systems coming online. I needed the speed, accuracy and repeatability of machine testing, and the ability to scale while not being reliant on a single penetration tester."

Solution

The emergence of improved automation tools across a range of disciplines had not escaped Ward Able's notice. "We looked at AttackIQ, and Advantage recommended it, which was good enough for us," he quips.

AttackIQ is an independent vendor of breach and attack simulation solutions and built the industry's first Security Optimisation Platform for continuous security control validation, improving security program effectiveness and efficiency. Its solutions are aligned with the MITRE ATT&CK framework. The MITRE ATT&CK framework is a knowledge base of tactics and techniques designed for threat hunters, defenders and red teams for attack classification, identification of attack attribution and objectives, and assessing risk.

Ward Able says demonstrations clearly showed the value of AttackIQ. "The customisation of the tool is phenomenal. It is easy to use with a great dashboard, and allows for testing against specific threats time and time again, using the techniques, tactics and protocols that hackers use to hack an organisation. You simply choose them from the MITRE ATT&CK framework."

He goes on to explain that Mitre 10 doesn't randomly test for various attacks, but instead narrows the field to the most likely sources and actors. "We use a lot of threat intel, so we know who is coming at us, who is more likely to be attacking. They generally have signatures as to how they would attack and we can test for that with AttackIQ, so we're essentially pretesting our systems for weaknesses against known threat actors," he explains.

As an example, Ward Able points to the recent spate of Lockbit ransomware attacks around the world. "We ran an AttackIQ scenario using Lockbit technique, tactics and processes against our systems. We then got a recommendation report out of AttackIQ saying this is where your systems would fail to detect or stop Lockbit from getting in, and this is what is required to harden those defences."

Results

Using smart tools is a highly effective approach, says Ward Able. "Instead of trying to boil the ocean with already overburdened security teams, we can focus in and work with our DevOps guys to put in fixes proactively, knowing we were likely to be a target."

He adds that Mitre 10 looks to partners like Advantage for supplementary resources. "We run a small security team and depend heavily on our partners for support. An example is curated testing, where a team of professionals from Advantage run the AttackIQ scenario against us, we agree on which systems are going to be hit, and the technique, tactics and processes to be used and which attack vector we're testing against. We run that against our systems, with a red team hitting us every month."

In these exercises, Ward Able says, Mitre 10's team leans on Advantage's capabilities. "That takes pressure off my security team, and it enhances the capabilities of our Security Operations Centre (SOC)."

Advantage | Mitre 10 | AttackIQ - Case Study

Owing to the random nature of cyberattacks, there are further ways to keep the SOC on its toes. “In some cases we let the SOC team know we have a pen test underway and what to expect; in other instances we just don’t tell them and wait to see their responses,” he explains, adding that this is “an interesting way to conduct live testing. We’ve found it to be really good, as it exposes weaknesses. If there is an area we expect to be monitored by the SOC and they don’t get an alert, we know there is a breakdown and we can sort it out.”

In addition to the AttackIQ service, Ward Able says monthly meetings with the Advantage team provides ongoing value. “They show evidence of where our controls are effective, and where they might need hardening or a bit of work; we take a lot out of that, using the knowledge from their team for our internal team and testing regimes, where we test systems again and again and again, so what we think is in place stays in place and we don’t drift from a hardened posture.”

He says Mitre 10 is working at bringing continuous security assurance into all functional systems, something AttackIQ is well-suited to. “You want effectiveness. When delivering fixes you need to retest and know that the hardening is effective and it stays fixed. With a manual pen test, you do it at a point in time and then only test again in the next quarter or 6 months later. Automated testing provides repeatability so we continuously test ourselves and nothing is left to chance. That is what we have and this is why it makes a difference.”

Finally, Ward Able asks himself a question, and answers it. “Is it expensive? No. Compared to manual pen testing, we were doing 4 per year against a single system. For same price, we now getting as many tests as we want in a year for the same price and we’re running them as often as possible on as many systems as possible.”

He has no hesitation in recommending Advantage and AttackIQ. “With security, there is no competitive advantage. It is about keeping one another safe.”