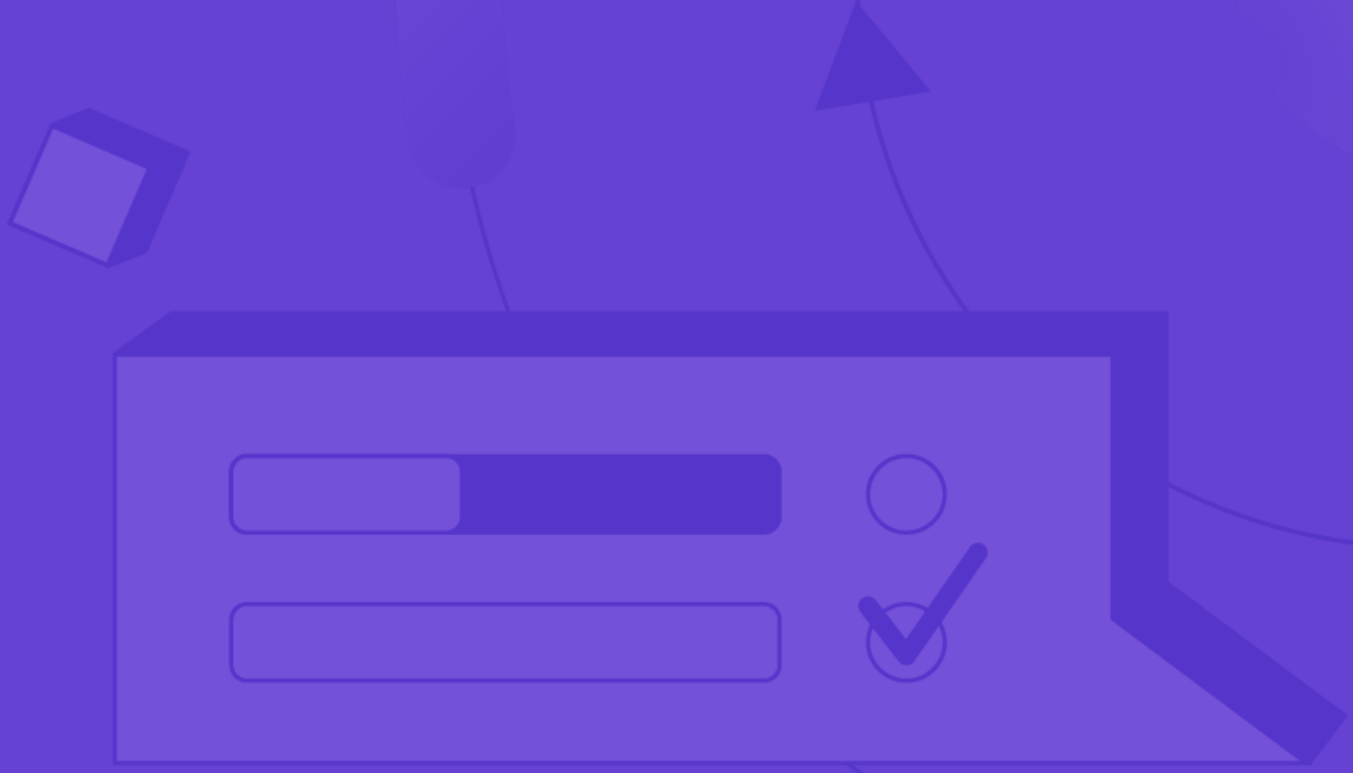
ATTACKIQ® + SA Power Networks

Case Study

SA Power Networks, an Australian Energy Company, Improves Security Control Validation and Reduces Costs with AttackIQ



SA Power Networks is South Australia's regulated electricity distributor supplying about 1.7 million people and leading a rapid transition to a net-100% renewable energy system in the State. SA Power Networks is always seeking to build a more sustainable, efficient, and innovative business that creates real value for customers.

Its role as an essential service provider to households and businesses across the State means, SA Power Networks supplies power to approximately 900,000 households and businesses in the state of South Australia. The company employs 2,000 people and is the sole electricity supplier for the region.

As a Critical Infrastructure (CI) provider in Australia, cybersecurity is a major consideration for the organization. Nathan Morelli, Head of Cyber Security, and IT Resilience at SA Power Networks, explains: *"We need to know we have done enough to protect the business and the State's electricity network from cyber threats. That means ensuring we have the right controls in place and that they are capable of helping us identify and respond to the most up-to-date and advanced threats."*

The 22-person strong security team has set itself the goal of preparing to defend against the top ten threats most likely to face the organization. The team identified these threats using the MITRE ATT&CK® framework, a knowledge base of adversary tactics and techniques derived from real-world observations. Leveraging the intelligence in MITRE ATT&CK, SA Power Networks' objective is to prevent and minimize the impact of attackers if they can breach their defenses. The company set out with the key question of: *"How can we do proactive, operationalized testing of our defenses?"*

> *"The value of AttackIQ is clear to see: a solution that allows us to detect advanced threats and show our controls are working, with ongoing posture validation replacing our expensive and limited penetration testing. As a Critical Infrastructure organization, the benefits of the approach are clear."*
>
> – **Nathan Morelli,**
> Head of Cyber Security and IT Resilience, SA Power Networks

CUSTOMER

SA Power Networks

LOCATION

Australia

INDUSTRY

Energy

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Automated Security Control Validation
- AttackIQ Vanguard Security Validation Service
- Threat Hunting
- Threat-Informed Defense

BUSINESS IMPACT

- Enabled a threat-informed approach to defense
- Replaces ad hoc penetration testing with continuous assessment and evaluation
- Significant cost savings per year in overheads associated with penetration testing
- Reduces log retention costs by 10% through more effective targeting of threats
- Enables security team to better manage security risk

Adopting a Threat-Informed Defense Strategy

To meet its security challenges, SA Power Networks has adopted an intelligence-led, threat-informed strategy that matures its cyber defense approach.

Morelli describes the situation: *"Our legacy approach was more reactive. When a security alert came through, all we could do was check our logs for indicators of a compromise. This intelligence is of limited value. Even evidence of a web shell doesn't tell you whether there was an actual breach. We needed to be at the front end of the attack and on a more proactive footing."*

The internal penetration tests conducted by the security team were also sub-optimal. Given the time and cost involved, such tests were ad hoc and usually focused only on a specific application rather than the entire enterprise IT infrastructure. The security team wanted to move to continual testing of the company's baseline security posture to ensure the highest levels of protection at any given time. It was at this moment that the company came across AttackIQ.

Automating Security Control Validation

Following a pilot phase, SA Power Networks deployed the AttackIQ Security Optimization Platform, which assesses security controls and validates that they are working as intended. The platform emulates the adversary with realism to assess security programs in a continuous and automated manner using scenarios and attack graphs aligned to the threat intelligence and adversary behaviors in MITRE ATT&CK.

Adopting the AttackIQ Security Optimization Platform was a *"no brainer,"* Morelli says. *"The value of AttackIQ is clear to see: a solution that allows us to detect advanced threats and show our controls are working, with ongoing posture validation replacing our expensive and limited penetration testing. As a Critical Infrastructure organization, the benefits of the approach are clear."*

Recently, the company has also adopted AttackIQ Vanguard, the company's co-managed security validation service, which ensures that SA Power Networks is getting the most value possible out of the AttackIQ Security Optimization Platform. With Vanguard, AttackIQ's experienced team of cybersecurity practitioners investigates and advises on the potential cyberattacks in SA Power Networks' environment using the platform to help achieve cybersecurity readiness.

"Our team is relatively small," says Lindbergh Caldeira, Cyber Security Operations Manager at SA Power Networks, *"so Vanguard will prove invaluable for us. With AttackIQ as our trusted partner, we can rest assured that we are getting the most out of the platform."*

Keeping a Lid on Cyber Risk

Armed with the AttackIQ Security Optimization Platform, SA Power Networks is now able to realize its threat-informed defense strategy in full. The platform provides evidence that the controls, configurations, and baselines put in place by the security team work as required. This helps the SA Power Networks make the most of all its investments across the security organization.

Nathan Morelli comments: *"AttackIQ gives us the ability to assess against our key threats, and that gives me the information I need to report to key stakeholders, such as the CIO or operations leads, that we are as secure as can be expected. Essentially, AttackIQ gives me the information I need to say with confidence that the programs and reporting we have in place are working to lower our cyber risk."*

> ***"AttackIQ Vanguard will prove invaluable for us. With AttackIQ as our trusted partner, we can rest assured that we are getting the most out of the platform."***
>
> – **Lindbergh Caldeira,**
> Cyber Security Operations Manager, SA Power Networks

Prioritizing Security Efforts

Before working with AttackIQ, SA Power Networks took a less organized approach to security control management, whereby it tried to address every control gap. Based on the intelligence provided by the AttackIQ Security Optimization Platform, the company can now prioritize its efforts according to its biggest security control gaps and emerging threats, which is particularly important as the IT team looks to innovate and bring in new digital systems. *"We now can act according to what the intelligence tells us for a true, risk-based approach. And the icing on the cake is that the platform aligns with MITRE ATT&CK. That alignment makes our jobs much easier and saves time and effort as everything is automated,"* adds Caldeira.

The depth of the insights revealed through the platform's breach and attack simulation (BAS) capabilities has proven particularly useful to the business. *"With traditional penetration testing we could discover perhaps one way into the network,"* explains Caldeira, *"but with AttackIQ we're given granular details on how various parts of an execution unfold using its attack graphs. This is much more beneficial to us as we can ensure our controls are effective across all dimensions of impact and it allows us to rapidly check our security posture against new, headline-grabbing threats and remediate where necessary."*

In addition to creating a more detailed and continuous approach to assessing security controls, AttackIQ is also saving the company significant costs per year by offsetting the costs of penetration testing. The company has realized further efficiencies as it no longer needs to send as many SIEM (security information and event management) or SOC (security operations center) logs into its pay-per-use cloud environment. This is because with AttackIQ, the company need only focus on the attacks most relevant to its business. It only needs to send logs relating to those specific tactics and techniques into the cloud, a benefit that is expected to reduce storage costs by approximately 10 percent.

Seamless Integration with Security Systems

One of the key use cases for AttackIQ is to ensure that SA Power Networks' cybersecurity tools are delivering value relative to their cost. The AttackIQ Security Optimization Platform integrates with key security tools such as its EDR (endpoint detection and response) systems, allowing the security team to evaluate how these systems respond to attack scenarios.

Where systems do not respond as expected, or where vendors have switched off certain capabilities, SA Power Networks can now raise these issues with the vendor. *"Often the issue comes down to a business value proposition risk,"* says Morelli. *"We've seen that vendors will turn off certain capabilities because enabling them risks the performance of our business. With these insights, we can now make better risk-informed decisions and understand where and why exemptions are in place and what further activities we may need to take to shore up our security as a result."*

Conclusion: Keeping the Lights on for Australia's Critical Infrastructure

In protecting a CI business, the objective of SA Power Networks security team is to keep the lights on for South Australians. For Nathan Morelli, the way they do that is by understanding the threats facing their business and the corresponding controls they have in place. *"That's what's great about AttackIQ,"* Morelli concludes, *"it allows us to identify our biggest potential security control gaps and gives us the visibility we need to ensure our controls are up to scratch. The AttackIQ Security Optimization Platform is therefore a fundamental layer of our threat-informed defense."*

ATTACKIQ

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