noname

Leading Telco in Asia

The telecommunications industry across Asia has seen rapid growth and development in recent years. This growth is largely due to the proliferation of mobile devices and increasing demand for better digital services. To meet this frenzy head-on, telcos are investing heavily in developing new technologies and expanding their networks to meet customer needs. As such, it's important to note that APIs, or Application Programming Interfaces, provide the necessary connectivity for this digital transformation and expedite DevOps processes.

Thanks to the power of APIs, many companies are now offering mobile phone services, internet access, and other telecommunication products to customers around the continent. These services are becoming increasingly popular due to their convenience and affordability. Furthermore, with the help of APIs, service providers are able to offer more personalized solutions and ultimately improve the customer experience.

One of the leading telcos in the region also sees this as a great opportunity for service providers to offer new digital voice and data solutions. And as the 5G era approaches, they have set their sights beyond telephony and onward to Big Data, AI, IoT and other emerging digital applications.

However, they also understand that while APIs are a huge win for our digital economy, their growing popularity also means the API attack surface is expanding at the same pace. Which is why the telco turned to Noname Security. They wanted to avoid the fate Australian telco Optus, Canadian telco Telus, and several other big name service providers faced in 2022 and the first quarter of 2023.

Problems

As with most of our customers, the most prevalent underlying vulnerability affecting organizations is the lack of visibility. Regardless of their company size or API footprint, on average, we discover 40% more APIs than the customer originally anticipated. And unsurprisingly, our API discovery module produced a similar outcome with this particular customer as well.

Prior to Noname, the extent of the customer's API security controls consisted of a legacy API management platform and an F5 web application firewall (WAF). From an application security and API delivery perspective, there is absolutely nothing flawed about this arrangement. However, neither are designed to provide the security controls and observability required to adequately protect APIs. This is because not all APIs are routed through a proxy like a WAF or API gateway.

But even with an accurate audit of their API inventory, the telco would still be shorthanded in terms of securing APIs during their normal functioning as they operate and manage requests. Quite simply, it would be impossible for their security teams to manually identify malicious behavior in their environment.

There are hundreds, if not thousands of API endpoints that need to be protected in real-time. Traditional AppSec solutions simply cannot keep up with all of the API calls within the customer's environment, leaving their environment vulnerable to cyber attacks without the proper runtime protection capabilities.

Solutions

The first phase of the engagement entailed a pilot deployment to locate telco's internal APIs, assess configurations, and understand the types of data traversing the APIs. The customer was immediately impressed with the speed in which the discovery was executed, the accurate inventory findings, and the sensitive data exposure the tool identified.

Due to the notable success of the pilot, the customer then expanded the coverage area of the Noname API Security Platform to their entire internal and external API estate. This exercise also revealed more hidden production APIs, and uncovered the most imminent threats facing their environment.

We found that the customer was defenseless against major security vulnerabilities like Broken User Authorization and Excessive Data Exposure. These are two of the top three API security risks as noted in the Open Worldwide Application Security Project (OWASP) API Security Top 10.

Equally important to these shadow API discoveries and reconfigurations was protecting the APIs from future attacks. With Noname deployed, the customer can now detect suspicious behavioral anomalies and trigger incident response protocols. The best part about it, it can all be done in real-time.

The customer doesn't need to rely on delayed reporting and access logs to inform the remediation process. Once suspicious behaviors are detected with the Noname platform, they are reported to the customer's API gateway, SIEM system, and other information security engines to inform the entire security team. The customer can choose to have their staff remediate the issue(s) manually, semi-automatically, or fully automatically depending on the use case and severity of the vulnerability.

Results

With the amount of data being transferred and stored by telcos on a daily basis, it's important to ensure that all of this information remains secure and protected. This entails adopting key API security measures around authentication, authorization, encryption, access control, and more.

By implementing these measures through a comprehensive API security platform, service providers can protect against data breaches and ensure their customers' data is safe from malicious actors. For this reason, Noname Security is trusted by the leading enterprises and iconic brands because we understand just how paramount data security is, and reliably deliver on our promise to global service providers.

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371