Securing Security

A prominent Australian Government Agency has a key role in Australia's cyber defence, providing monitoring, advice and information to individuals, businesses and critical infrastructure operators.

Over the past few years, networks have been radically transformed.

Traditional network perimeters have been replaced with multiple edge environments, multi-cloud, remote worker, Internet of Things (IoT), mobile devices, and more, each with its unique risks and vulnerabilities.

One of the most significant advantages to cyber criminals is that all these edges are interconnected as applications and workflows move data between environments. Organizations have often sacrificed centralized visibility and unified controls to leverage the performance and agility of this new world.

An Australian Government Agency has been formed to lead the Australian Government's efforts to improve cyber security. Their role is to help make Australia the most secure place to connect online.

They monitor cyber threats across the globe 24 hours a day, seven days a week, to give Australians early warning of an incident.

The agency provides a call centre offering advice and information on cyber protection and when there is a cyber security incident, they provide clear and timely advice to individuals, businesses and critical infrastructure operators.

This critical call centre service has some unique challenges:

The ability to scale in the event of a cyber security incident

The need to protect itself from a denial of service attack

The ability to operate from anywhere, on any network at any time

Amazon Connect was selected as the solution to meet these requirements. One of the biggest challenges was how to evidence scalability, performance and security before moving this critical service into production.

Agency Goals

- Load test the cyber security contact center beyond expected peaks, replicating both normal caller behaviour and call patterns intended to disrupt the service.

- Measure and evidence the performance of the end-to-end environment from Customer to Agents

- A/B test production and disaster recovery (DR) environments, replicating the identical call scenarios.

"Operata's testing and assurance technology was critical in establishing and assuring the performance on our cyber security contact center."

Key Points

Cyber security has never been more important

An Australian Government Agency has a key role in Australia's cyber defence, providing monitoring, advice and information.

Their contact centre is a primary contact channel that needs to scale to meet the demands of a cyber security incident.

As well as reliability and scalability the service has unique requirements in the need to protect itself from a voice denial of service attack, which could be coordinated to increase the impact of a security event.

Government

"'As well as reliability and scalability the service has unique requirements in the need to protect itself from a voice denial of service attack, which could be coordinated to increase the impact of a security event'"

Project Manager, Systems Program Office

The Solution

The agency selected the Operata Assurance service to performance test and provide assurance to this new service.

Operata's expert services worked with their team to develop a series of test campaigns that would deliver real calls into their environment that replicated anticipated customer interactions (good and bad actors)

Specific requirements included:

- Test calls to be delivered using 600 unique 'from numbers'
- Variable call delivery rates of up to 15 calls per second
- Specific call delivery patterns to replicate denial of service scenarios
- Inbound carrier performance measurement
- Agent network and workstation performance measurement

Test agents, using the Salesforce Service Cloud Voice client to answer calls, had the Operata Agent Experience Collector for Chrome installed on their workstation, this captures both network and workstation performance as well as browser versions, softphone events, softphone logs/errors and agent actions.

Over a two week period 70,000 test voice minutes were delivered into the agency's Amazon Connect contact center environment, with over 4 million performance measures and 2,300 Softphone events captured within the Operata platform.

As the campaigns progressed the Operata platform provided real-time insights, highlighting anomalies and allowing their team to establish the cause issues often before the campaign completed.

Once completed, call and agent performance measures, as well as the call recordings were all exported from the Operata platform to quickly provide the supporting test reports.

All Issues encountered during the initial campaign runs were either resolved or escalated to third parties.

As the testing plan progressed confidence grew in the performance of the service with all elements operating well within expected thresholds.

On completion the team and their business had both witnessed and had evidence to be confident in moving to the next stages of offering this service to the general public.

Operata Solution

- Performance Monitoring
- Assurance
- Call Timeline & Agent Status
- Insights & Analytics

operata.com