

Cyber Security 2022 Federal Election



The Australian Electoral Commission (AEC) is the Commonwealth agency responsible for conducting Federal Electoral Events and maintaining the Commonwealth Electoral Roll. As the entity trusted to manage the election process, count the votes, and declare results, the AEC fulfils a critical role supporting Australian democracy. A rapidly evolving and aggressive cyber threat environment coupled with constant cyber-attacks in Australia and overseas, have highlighted the importance of maintaining the integrity of electoral IT systems and protecting them against interference. Ensuring public confidence in the integrity of the system is critical.

High stakes security requirements

To supplement existing capabilities within the AEC's Cyber Security division, the AEC sought to engage an experienced service provider to rapidly enable a cloud based Cyber Security Monitoring Solution (CSMS). The solution had to be agile and scalable, with the ability and capacity to expand and contract IT resources based on AEC's requirements for major events such as the Federal Election. The ability to leverage trends in cloud and cyber security were also important to ensure electoral integrity immediately and into the future.

The key to success: robust people, process, and technology

AUCloud's ability to deliver a superior technical solution, expertise operating a highly secure cloud environment coupled with a strong security focused governance framework, positioned AUCloud well to meet the AEC's requirements.

From the outset, AUCloud engaged openly and collaboratively with the AEC. This ensured early identification and resolution of issues and enabled

- AUCloud to be responsive to the AEC's requirements,
- including where these matured as the project progressed.

Central to the solution was the e2e-assure Cumulo platform. A world leading cloud-based cyber defence and protective monitoring technology, Cumulo uses in-house, commercial, and open-source security monitoring applications to provide a complete Security Operations Centre as a Service platform. With capability including device log monitoring, intrusion detection, risk analysis and threat intelligence, the solution scales in response to the threat landscape and the needs of the customer.

However, the overwhelming strength of the solution lies in the team of onshore highly skilled, experienced and security cleared AUCloud SOC analysts, that complement the technology to enable informed response capability. Leveraging the platform and working in close partnership, AEC and AUCloud cyber security specialists could rapidly identify, analyse, risk assess and respond to potential threats before they became incidents – all in real time.

Australia's Democracy

Engineered to PROTECTED, and with the ability to adapt service levels and response times, AUCloud's solution has delivered the flexibility to support AEC's business as usual activity, as well as heightened monitoring and activity such as during the 2022 Federal Election. With the ability to scale as the business need demands AEC has confidence that instant capability to meet variable operational priorities is available at their fingertips. When it mattered most – during the Federal Election - the ability to integrate multiple toolsets to gain a superior level of situational awareness through a single pane of glass proved invaluable to AEC's ability to access the intelligence required to make informed decisions and respond rapidly.

The integrated nature of the solution (monitor, detect and respond to cyber incidents), augmented by the skills transfer of AUCloud's expertise to the AEC team, has also armed AEC with new capability. With electoral systems fully monitored with use cases and playbooks to investigate and respond to incidents as they arise, AEC benefits from being both proactive and well prepared – managing risks to avoid incidents and provide real value back to the business.

Because the solution is cloud-based, management, maintenance and capacity are included in the service; avoiding the high engineering and maintenance overheads typical of traditional models, and because the AUCloud solution uses standard toolsets and maximises native logging capabilities within AEC's existing operating systems, there is no 'lock-in' should AEC's needs change in the future.

“ The AEC is very appreciative of the services provided by AUCloud and the Cyber Security Monitoring Service (CSMS) they deployed to support the secure delivery of the Federal Election. Cyber security is obviously a significant risk for any organisation and ensuring the integrity of our electoral processes is paramount to the work that we do at the AEC. AUCloud's team of cyber security professionals were great to work with – trustworthy, experienced, highly professional and most importantly responsive to our needs and that of a dynamic cyber security landscape. AUCloud played a key role in ensuring our success and helping the AEC defend democracy.

Matthew Haigh,
Australian Electoral Commission
Chief Information Security Officer



Benefits

- ✓ Additional assurance around the confidentiality, integrity, and availability of Australia's electoral events
- ✓ Improved situational awareness allows confident decision making and reduces risk
- ✓ Ability to triage and analyse threats before they become incidents
- ✓ Real time capability to investigate anomalous events/incidents
- ✓ Responsive scalability
- ✓ Knowledge and skills transfer
- ✓ Confidence that all data, including metadata, support, and analytics data stays in Australia
- ✓ Geo-resilience across multiple Certified Strategic data centre zones
- ✓ Flexible and adaptive subscription-based payment model

Contact

1800-282-5683
sales@australiacloud.com.au
australiacloud.com.au

Data
security is
our DNA

