Securing Australia's cyber skill war chest

Canberra based SME FifthDomain delivers highly tailored and sophisticated cyber training. Using a range of learning and exercise modes, FifthDomain provides hands on operational, cyber security skills development. Simulating threat environments, FifthDomain can measure and analyse the skills of individuals and provide personalised training to meet the specific cyber security needs of an organisation.

The search for a homogeneous technical solution

The rapidly evolving cyber threat environment is constantly driving demand for equally sophisticated cyber security capability. The vision when establishing FifthDomain was to build a highly advanced and agile cyber training solution tailored to the changing cyber landscape and skill demands of organisations. This meant addressing the complex challenge of physically setting up and configuring multiple online learning environments, premised on different content and training models to meet the different skill needs of customers.

Early success was achieved leveraging a cloud based Open Stack technology approach, challenges emerged as the business scaled. Different versions of technology combined with the effort associated with individualised code adjustments to support different customers, scenarios and environments, required a more homogenous technical solution. The objective: to streamline and improve the efficiency of business operations whilst delivering superior quality, tailored learning experiences and outcomes for customers.

The solution also needed scale capability and ideally, align with the technology stacks used by their customers – primarily government.

Already a sophisticated virtual technology user itself, FifthDomain wanted an infrastructure provider that could match its operational pace, technical knowledge and ambition for growth.

Tailoring IaaS for tailored services

Being a sovereign cloud IaaS provider AUCloud immediately satisfied one of FifthDomain's core criteria. Recent assessment of AUCloud's security status to the PROTECTED level controls of the Australian Cyber Security Centre's (ACSC) Cloud Assessment and Authorisation Framework (CAAF), further validated AUCloud's focus on security and its cadence on aligning with the rigorous security requirements of government.

Importantly, because AUCloud demonstrated compliance with the sovereignty requirements of the CAAF, i.e., that the business was owned, operated and managed in Australia by security

> " Transitioning to the AUCloud IaaS is foundational to growing the business and providing the sophisticated cyber security skill training Australia needs to keep pace with the changing cyber landscape. The ability to rapidly tailor and provision VMs, not just 10s and 100s but literally 1,000s of VMs rapidly is a game changer. We can do more, more quickly and with less time-consuming effort with certainty that we can respond to the training needs of our customers. "
>
> **Matt Wilcox,
> CEO and Founder, FifthDomain**

cleared Australian personnel, FifthDomain and their customers had certainty their data would always remain onshore and not at risk of access or interception by foreign nationals.

AUCloud's technology choices in building their IaaS were also critical. Because AUCloud's IaaS is deployed on a VMware based technology suite, the predominant technology used across government and their many legacy systems, technology alignment with customers was achieved. Not only could training environments mirror the in-house operations of customers, but modules could be tailored to hone the skills that individuals would use on a day to day basis in their home agency.

While FifthDomain often needs to support operational training environments for large numbers of users, this may only be for the few hours a week the customer uses the service. The ability to scale up and down based on demand was therefore also critical.

Outcomes

From the outset, working collaboratively with the AUCloud Development Team accelerated the setup process enabling FifthDomain to ramp up quickly. Once operational, FifthDomain immediately

realised value with the ability to rapidly provision VMs for customised events. In one instance, the task of building and customising a training environment that typically took a week of effort, was delivered within a couple of hours. In another, using AUCloud's automation and orchestration FifthDomain had the capability at hand to dynamically respond to the variable demand for VMs used for a cyber event involving a large number of geographically dispersed, intensive users over a period of a couple of days. With over 5,000 VMs available, scale could be adjusted as required.

Access to AUCloud's Infrastructure-as-Code has also enabled FifthDomain to write code directly to their platform, giving them additional flexibility and control to build and manage their environments.

With the ability to also scale back and turn off VMs not in use, FifthDomain only pays for the capacity it uses. This delivers efficiencies and enables costs to be controlled.

Benefits

- ✓ Technology alignment with government customers
- ✓ Responsive scalability and elasticity of IaaS resources
- ✓ Ability to write code directly to the infrastructure (infrastructure as code)
- ✓ Only required to pay for what they use

- ✓ Streamlined and efficient set up and delivery
- ✓ Highly secure, sovereign environment to protect sensitive cyber training and skills data
- ✓ Confidence that all data, including metadata, support and analytics etc data stays in Australia – always

Contact

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